Numer 4/2021 (39)
ISSN 2720-0604

DLP expert

Data Leak Prevention

www.dlp-expert.pl

Powrót do biura: jak zadbać o cyberbezpieczeństwo podczas powrotu personelu do pracy stacjonarnej

Dlaczego cyberbezpieczeństwo stanowi najwyższy priorytet dla infrastruktury przemysłowej

BGP, DNS i kruchość naszych systemów krytycznych

Chmura nad Wisłą – tak, ale powoli

Jak przetestować plan usuwania skutków katastrofy, a przy okazji cały zespół

DLP Expert
kwartalnik
numer 4/2021 (39)
styczeń 2022

ISSN
2720-0604

Wydawca
DLP Expert Sp. z o.o.
ul. Leszczyńskiego 4 lok. 25
50-078 Wrocław
tel. 71 722 76 15
fax: 71 735 18 82
e-mail: redakcja@dlp-expert.pl
www.dlp-expert.pl

Przygotowanie DTP
Batorski Poligrafia
www.batorski.pl
firma@batorski.pl

Redaktor naczelny
Piotr Domagała

Redaktor techniczny
Grzegorz Grodzki

Zachęcamy do lektury kolejnego zeszytu DLP Expert-a. Jak zawsze, poruszamy w nim problemy związane z cyberbezpieczeństwem. Staramy się przy tym, aby poruszane tematy były nie tylko ciekawe, ale przede wszystkim aktualne. Mamy głęboką nadzieję, że również i tym razem znajdą Państwo tu wiele interesujących informacji ze świata IT.

W aktualnym numerze zamieściliśmy zarówno bieżące raporty o stanie zagrożeń, opracowane przez specjalistów z tak znanych firm jak Kaspersky, F5, OVHCloud, Fortinet, Sophos czy innych. Ponadto jest tu szereg artykułów dotykających różnych problemów branży IT. Można tu wymienić m.in. problemy z powrotem do pracy stacjonarnej po pandemii, ochronę infrastruktury przemysłowej, kruchości systemów krytycznych a także o spowolnieniu rozwoju chmury w naszym kraju.

Nie można pozostawić także bez komentarza ciągle roztrząsanych problemów związanych np. z ransomware i jego ewolucją, kwestiami elementarnymi ale niezwykle ważnymi dla naszego bezpieczeństwa czyli kopiami zapasowymi, politykami tworzenia kopii czy testowania opracowywanych planów odtwarzania itd.

Polecamy również tekst Stormshield, którego autorzy dotykają problemu ochrony zasobów wodnych w Polsce, prezentowany artykuł przytacza szereg przykładów udanych ataków na tego typu infrastrukturę na świecie.

Zapraszamy do lektury
Redakcja DLP

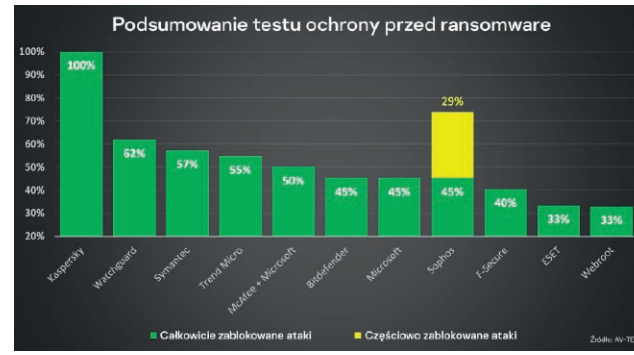
Spis treści

Kaspersky Endpoint Security Cloud wykrywa 100% zagrożeń ransomware w badaniu AV-TEST

5.10.2021 r. - Kaspersky Endpoint Security Cloud wykazał 100% skuteczność w zwalczaniu ataków ransomware – wynika z oceny przeprowadzonej niedawno przez niezależną organizację AV-TEST. Produkt został przetestowany przy użyciu trzech różnych scenariuszy oraz 113 próbek ataków i nie dopuścił do utraty żadnego pliku użytkownika, radząc sobie lepiej niż 10 pozostałych dostawców rozwiązań cyberbezpieczeństwa.

W ciągu ostatnich kilku lat wokół oprogramowania ransomware rozwinął się cały przemysł: pojawiło się wiele rodzin tego typu szkodliwego oprogramowania, wyspecjalizowanych cybergangów oraz ataków w formie usługi. Tylko w drugim kwartale 2021 r. badacze z firmy Kaspersky zidentyfikowali niemal 4 tysiące nowych modyfikacji oprogramowania ransomware oraz ponad 97 tysięcy ataków na użytkowników na całym świecie – o 6 tysięcy więcej niż w poprzednim kwartale. Po uzyskaniu dostępu do systemu szkodliwy program ransomware szyfruje lub w inny sposób blokuje dostęp do danych i żąda zapłacenia okupu. Wiele szkodników tego typu potrafi szybko rozprzestrzeniać się z jednej maszyny na kolejną w sieciach firmowych, a usunięcie skutków ataku oraz odzyskanie plików może trwać kilka dni, a nawet miesięcy. W celu uniknięcia dotkliwych oraz kosztownych skutków takich ataków firmy powinny stosować sprawdzone i niezawodne rozwiązanie cyberbezpieczeństwa, które potrafi wykrywać szkodliwą aktywność oraz wycofywać działania związane z szyfrowaniem.

Niezależna organizacja AV-TEST zbadała 11 rozwiązań do ochrony punktów końcowych w trzech scenariuszach z wykorzystaniem szkodliwych programów ransomware: ataki na pliki użytkowników przechowywane w systemie lokalnym, ataki na pliki użytkowników przechowywane w zdalnym, współdzielonym folderze oraz ataki przy użyciu nieznanych zagrożeń. Podczas badania produkty miały za zadanie wykryć aktywność oprogramowania ransomware oraz jego pliki, zablokować je, wycofać wszelkie zmiany w plikach użytkowników i wyeliminować zagrożenie z atakowanego systemu. Wykorzystano 25 rodzin oprogramowania ransomware, takich jak REvil, Ryuk, Conti, Lockbit, pysa, Ragnarlocker, Ransomexx itd., jak również 14 nieznanych zagrożeń.



Ochrona przed ransomware oferowana przez różne produkty wg AV-TEST. „Całkowicie zablokowane ataki" oznacza wykrycie oprogramowania ransomware oraz ochronę wszystkich plików użytkownika. „Częściowo zablokowane ataki" oznacza wykrycie oprogramowania ransomware z utratą (brakiem ochrony) niektórych plików użytkownika.

Kaspersky Endpoint Security Cloud zablokował 100% ataków we wszystkich trzech scenariuszach, nie dopuszczając do zaszyfrowania ani jednego pliku użytkownika oraz skutecznie eliminując zagrożenia z chronionego systemu. Produkt firmy Kaspersky osiągnął najwyższy współczynnik ochrony ze wszystkich testowanych rozwiązań, wykazując swoją przydatność dla firm w zakresie obrony przed tego rodzaju atakami. Zdołał ochronić dane firmowe na atakowanym komputerze pracownika, jak również pliki znajdujące się we współdzielonych folderach zainfekowanych istniejącymi rodzinami oprogramowania ransomware oraz próbkami stworzonymi specjalnie na potrzeby testu. Te ostatnie wykorzystywały różne rzeczywiste techniki szyfrowania stosowane przez cyberprzestępców.

Pełny raport opracowany przez organizację AV-TEST jest dostępny na stronie https://r.kaspersky.pl/x1VXs.

Uwierzytelnianie wieloskładnikowe ma znaczenie: duży wzrost liczby użytkowników atakowanych trojanami kradnącymi hasła

11.10.2021 r. - Cyberprzestępcy nieustannie wymyślają nowe mechanizmy oszustw online, a ostatnie sześć miesięcy charakteryzowało się istotnym wzrostem takiej aktywności. Badacze z firmy Kaspersky obserwowali zwiększoną liczbę ataków, w których cyberprzestępcy wykorzystywali trojany kradnące hasła dostępowe do usług online i inne informacje o kontach użytkowników.

Badacze z firmy Kaspersky przeanalizowali okresy od stycznia do września z lat 2020 i 2021 pod kątem liczby prób infekcji i ofiar. Analiza wykazała istotny wzrost liczby atakowanych użytkowników. Na przykład we wrześniu 2021 r. odnotowano o 160 tysięcy ataków więcej niż w kwietniu tego samego roku, co daje wzrost na poziomie 45%.

W ostatnich miesiącach eksperci zauważyli także gwałtowny przyrost liczby prób infekowania użytkowników – o niemal 30% w okresie lipiec-sierpień. Łączna liczba wykrytych prób ataków zarejestrowanych od stycznia do września 2021 r. wyniosła 24,8 mln – o 0,7 mln więcej niż w analogicznym okresie w ubiegłym roku.

MysterySnail: Kaspersky wykrywa atak wykorzystujący lukę dnia zerowego systemie Windows

13.10.2021 r. - Pod koniec lata 2021 r. technologie wykrywania firmy Kaspersky zapobiegły serii ataków na serwery działające pod kontrolą systemu Microsoft Windows, w których wykorzystywano szkodliwy kod umożliwiający zwiększenie uprawnień w infrastrukturze ofiary. W wyniku dokładniejszej analizy incydentu badacze z firmy Kaspersky wykryli nowe szkodliwe narzędzie wykorzystujące lukę dnia zerowego w systemie Windows.

W pierwszej połowie roku eksperci z firmy Kaspersky zaobserwowali wzrost[1] liczby ataków wykorzystujących luki dnia zerowego, czyli nieznane dotąd błędy w oprogramowaniu, które zostają wykryte przez cyberprzestępców, zanim zrobi to dostawca oprogramowania lub badacze bezpieczeństwa. Ponieważ dostawca nie jest świadomy występowania takiej luki, nie są tworzone poprawki w celu jej usunięcia, a tym samym prawdopodobieństwo powodzenia ataku wzrasta.

Technologie firmy Kaspersky wykryły serię ataków na licznych serwerach działających pod kontrolą systemu Microsoft Windows, w których wykorzystano szkodliwy kod umożliwiający podniesienie uprawnień. Kod tego narzędzia posiadał wiele podobieństw do starszego, powszechnie znanego exploita, wykorzystującego lukę w zabezpieczeniach CVE-2016-3309[2], jednak dokładniejsza analiza przeprowadzona przez badaczy z firmy Kaspersky wykazała, że mają oni do czynienia z nowym exploitem dnia zerowego, któremu nadali następnie nazwę MysterySnail.

Na podstawie podobieństwa kodu oraz faktu ponownego wykorzystania tej samej infrastruktury sterowania badacze powiązali te ataki z ugrupowaniem IronHusky oraz chińskojęzyczną

aktywnością cyberprzestępczą sięgającą wstecz aż do 2012 r.

Badając szkodliwe funkcje wykorzystywane wraz z nowym dnia zerowego, badacze z firmy Kaspersky ustalili, że warianty tego szkodnika były wykorzystywane w przeprowadzanych na szeroką skalę kampaniach szpiegowskich przeciwko firmom IT, dostawcom z branży wojskowej i obronności oraz placówkom dyplomatycznym.

Luka została zgłoszona firmie Microsoft i doczekała się poprawki 12 października 2021 r. w ramach październikowej „środy poprawkowej".

Produkty firmy Kaspersky wykrywają exploita wykorzystującego wspomnianą wyżej lukę oraz powiązane z nim szkodliwe moduły, jak również zapewniają właściwą ochronę przed nimi.

Szczegóły techniczne dotyczące nowego exploita dnia zerowego są dostępne na stronie https://r.kaspersky.pl/6nwyv.

[1] *https://www.youtube.com/watch?v=5XcbZJnQJmo&t=242s*

[2] *https://github.com/siberas/CVE-2016-3309_Reloaded/*

Każdy mógł pobrać dane klientów sieci Plus

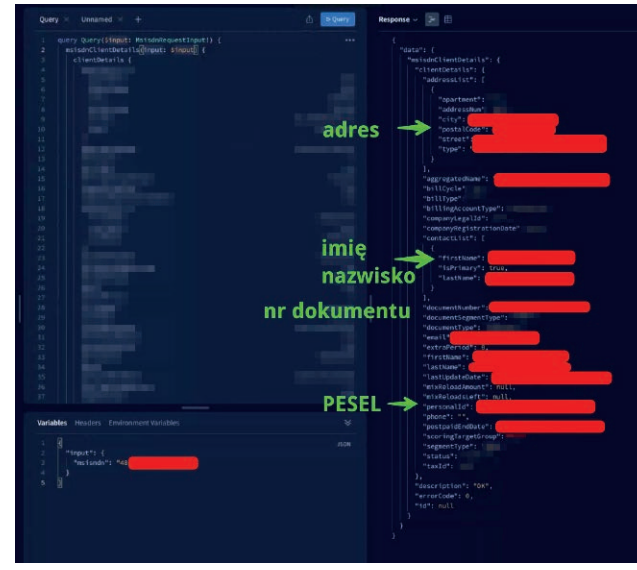
17.10.2021 r. - Jak informuje serwis niebezpiecznik.pl, każda osoba, która weszła na specjalną podstronę w domenie Plusa, mogła podejrzeć dane klientów tej firmy oraz jej drugiej marki, Plusha. Możliwe było ustalenie, do kogo należy dany numer telefonu, a także uzyskać dostęp do numerów PESEL, adresów zamieszkania i innych danych.

Dostęp przez niezabezpieczone API

Pobieranie danych klientów i zarządzanie innymi systemami wewnętrznymi Plusa i Plusha umożliwiało publicznie dostępne, niezabezpieczone żadnym tokenem API (czyli interfejs programowania aplikacji, służący programistom do wygodniejszego sterowania systemami informatycznymi). Firma Plus udostępniła swoje API bez żadnego zabezpieczenia pod następującymi adresami:

api.plus.pl/api

api.plushbezlimitu.pl/api



Zazwyczaj trzeba znać nie tylko adres takiego API, ale także nazwy metod (funkcji) i przyjmowanych przez nie parametrów. Nie zawsze łatwo jest je przewidzieć, ale w przypadku Plusa z pomocą przychodziła udostępniona dokumentacja, która bardzo precyzyjnie opisywała każdą z metod i przyjmowane przez nią argumenty. Na podstawie analizy dokumentacji można było zbudować zapytanie, które zwracało dane klienta dla podanego numeru telefonu, m.in:

- imię i nazwisko,
- adres zamieszkania,
- numer dokumentu,
- numer identyfikacyjny (PESEL) / nr dokumentu,
- adres e-mail.

Masowe pobieranie danych na temat klientów mogły utrudnić dwie kwestie:

- API zwracało odpowiedź lub pełne dane nie dla wszystkich numerów telefonów klientów Plusa (nie wszyscy musieli przecież podać np. adres e-mail),
- API nie zawsze zwracało dane szybko.

Operator ograniczył dostęp do metod API i usunął swojego klienta webowego wraz z dokumentacją, a całą sytuację wyjaśnił w przesłanym do redakcji oświadczeniu:

W jednym z naszych systemów teleinformatycznych wykryty został błąd związany z funkcjonowaniem API. Błąd ten wystąpił w związku z przeprowadzoną aktualizacją systemu. W jego wyniku istniała potencjalna możliwość uzyskania nieuprawnionego dostępu do danych zarządzanych przez spółkę. Luka umożliwiała wywołanie pojedynczych rekordów zawierających m.in. dane osobowe poprzez wykonanie odpowiedniego zapytania w API.

Luka w zabezpieczeniach została wykryta przez ekspertów, a nie przez hakerów. Zostaliśmy o niej poinformowani w poniedziałek, 11 października. Błąd został niezwłocznie usunięty, po kilkunastu godzinach, od 12 października nasz system jest odpowiednio zabezpieczony. W ostatnich dniach przeprowadzaliśmy kompleksowe testy i weryfikacje, które miały na celu sprawdzenie bezpieczeństwa systemu po wyeliminowaniu luki. Przebiegły one pozytywnie.

Po wnikliwej weryfikacji stwierdziliśmy, że nieznacznie zwiększona liczba wszystkich zapytań – o kilkadziesiąt sztuk – kierowanych do naszej bazy występowała od 5 października. Nie stwierdziliśmy, by w okresie istnienia luki miało miejsce masowe nieuprawnione odpytywanie o dane. Jedyne zarejestrowane zdarzenia związane z tym incydentem, zgodnie z naszymi ustaleniami na ten moment, dotyczą diagnozowania błędu przez ekspertów, którzy nas o nim poinformowali. Łącznie w tym okresie mówimy o kilkudziesięciu rekordach, których dotyczył nieautoryzowany dostęp.

W wymaganym przepisami prawa terminie zgłosiliśmy do UODO zaistnienie opisywanego błędu systemowego. Klienci, których części danych dotyczył nieautoryzowany dostęp, zostaną indywidualnie poinformowani przez naszą spółkę. Dane pozostałych naszych klientów są bezpieczne.

Pozdrawiam, Tomasz Matwiejczuk, Dyrektor ds. Komunikacji Korporacyjnej, Rzecznik Prasowy

Podsumowując, do odsłonięcia niezabezpieczonego API doprowadziła aktualizacja. Plus zobowiązał się do przeanalizowania logów związanych z działaniem API i skontaktowania się z klientami, których dane mogły zostać pobrane.

Jak twierdzi serwis Archive.org, API było publicznie dostępne już od co najmniej 15 czerwca 2021 roku. Niebezpiecznik przypomina, że dostęp do API daje nie tylko możliwość pobierania danych, lecz także ich zmiany lub tworzenia. A jak wynika z opisu niektórych metod w dokumentacji udostępnionej przez Plusa, część z nich — przynajmniej z nazwy — to takie metody, które dają możliwość sterowania treścią, jaka wyświetla się osobom odwiedzającym stronę internetową Plusa. Jak zapewnił operator: Nie było możliwości ingerowania w treści na stronie sklepu, ani podmiany elementów strony głównej.

Osoba, która uzyskałaby dostęp do modyfikacji treści stron internetowych operatora, mogłaby:

- podsłuchiwać wprowadzane przez klientów dane, np. hasła podczas logowania,
- podmieniać wprowadzane przez klientów dane, np. te dotyczące doładowania, przejmując je i okradając klientów,
- oszukiwać klientów, wyświetlając atrakcyjne, ale fałszywe promocje/bannery czy obiecując korzyści w zamian za np. jednorazową wpłatę przy pomocy karty płatniczej (wyłudzając w ten sposób dane karty płatniczej).

61 zaawansowanych taktyk w ewolucji trojana bankowego Trickbot

19.10.2021 r. - Głównym celem wykrytego w 2016 r. trojana bankowego Trickbot była kradzież danych bankowych online. Szkodnik ten zmieniał się na przestrzeni pięciu lat swojej aktywności w wyniku coraz bardziej zaawansowanego zestawu narzędzi tworzonego przez cyberprzestępców. Badacze z firmy Kaspersky prześledzili ewolucję Trickbota, analizując 61 jego dotychczasowych modułów, i ustalili, w jaki sposób cyberprzestępcy aktualizowali tego trojana.

Trickbot wywodzi się od trojana bankowego Dyre, który początkowo kradł dane bankowe oraz dane uwierzytelniające do kont e-bankowości. Szkodnik ewoluował do obecnej postaci wielomodułowego zagrożenia, którego zakres aktywności obejmuje obecnie wiele nowych funkcji, takich jak rozprzestrzenianie innych szkodliwych programów (np. ransomware Ryuk).

Badacze z firmy Kaspersky przeanalizowali łącznie 61 modułów Trickbota i odkryli, że trojan został zaopatrzony w dziesiątki modułów pomocniczych, których celem jest kradzież danych uwierzytelniających oraz wrażliwych informacji. Szkodnik rozprzestrzenia się za pośrednictwem sieci lokalnych, wykorzystując skradzione dane oraz wrażliwe informacje, zapewnia atakującym dostęp zdalny do maszyn ofiar, przeprowadza ataki siłowe

oraz pobiera inne szkodliwe oprogramowanie.

Trickbot atakuje firmy oraz użytkowników indywidualnych na całym świecie. Według badaczy z firmy Kaspersky aktywność trojana nie jest ograniczona geograficznie, a większość atakowanych użytkowników była zlokalizowana w Stanach Zjednoczonych (13,21%), Australii (10,25%) oraz Chinach (9,77%), a w mniejszym stopniu w Meksyku (6,61%) oraz Francji (6,30%).

Rozwiązania bezpieczeństwa firmy Kaspersky skutecznie wykrywają i blokują wszystkie znane wersje trojana bankowego Trickbot.

Więcej informacji na temat omawianego zagrożenia znajduje się na stronie https://securelist.com/trickbot-module-descriptions/104603/.

Ewolucja rosyjskojęzycznej cyberprzestępczości: co zmieniło się przez ostatnie lata?

20.10.2021 r. - Przez prawie dziesięć lat eksperci z działu badań incydentów komputerowych w firmie Kaspersky analizowali różne zdarzenia naruszenia cyberbezpieczeństwa, z których większość dotyczyła aktywności rosyjskojęzycznych cyberprzestępców. W ostatnich latach badacze zaobserwowali kilka istotnych zmian, jeśli chodzi o sposób działania tych cybergangów oraz ich najczęstsze cele.

Zrozumienie, w jaki sposób działają cyberprzestępcy oraz jak ewoluują pod względem taktyk, technik i procedur, jest niezwykle istotne w środowisku związanym z cyberbezpieczeństwem i pomaga osobom odpowiedzialnym za bezpieczeństwo korporacyjne lepiej przygotować się do obrony przed ewentualnymi incydentami. Dlatego eksperci z firmy Kaspersky pokusili się o przegląd najważniejszych zmian, jakie zaszły na przestrzeni ostatnich sześciu lat – a zmieniło się wiele.

Na przykład, nie są już powszechne tzw. ataki po stronie klienta, polegające na masowej infekcji przy pomocy szkodliwego oprogramowania kradnącego pieniądze z wykorzystaniem różnych luk w zabezpieczeniach popularnych przeglądarek. Kilka lat temu ten wektor infekcji był często wykorzystywany przez rosyjskojęzyczne cybergangi do atakowania określonych celów wśród organizacji handlowych i finansowych (na celowniku byli głównie pracownicy działów księgowości). Jednak od tamtego czasu twórcy przeglądarek oraz innych podatnych na ataki technologii online włożyli wiele wysiłku w udoskonalenie bezpieczeństwa swoich produktów i wdrożenie automatycznych aktualizacji. W efekcie przeprowadzenie skutecznej kampanii infekcji stało się trudne. Dlatego cyberprzestępcy uciekają się do precyzyjnych i spersonalizowanych ataków phishingowych, nakłaniając potencjalne ofiary do otwarcia szkodliwych załączników wykorzystujących lukę w popularnym oprogramowaniu, która – jak mają nadzieję przestępcy – nie została załatana na czas na atakowanym komputerze.

Inna istotna zmiana polega na tym, że cyberprzestępcy nie tworzą już własnego szkodliwego oprogramowania, jak miało to miejsce kilka lat wcześniej, ale wykorzystują publicznie dostępne narzędzia służące do testów penetracyjnych oraz zdalnego dostępu. Organizacje mogą używać takich narzędzi do legalnych celów, dlatego oprogramowanie bezpieczeństwa nie wykryje ich automatycznie jako szkodliwych. Właśnie na to liczą przestępcy. Korzystanie z narzędzi do testów penetracyjnych pomaga atakującym także zaoszczędzić mnóstwo zasobów, które musieliby przeznaczyć na rozwój własnych technologii.

Przestępcy aktywnie wykorzystują infrastrukturę publicznej chmury, zamiast tworzyć i obsługiwać własne zasoby. W połączeniu z możliwością wykorzystania gotowych narzędzi sprawia to, że atakujący nie muszą już budować i utrzymywać dużych gangów. Nastąpiła także znacząca zmiana w zakresie potencjalnych ofiar: z ataków na organizacje oraz instytucje finansowe na ataki z użyciem oprogramowania ransomware oraz mające na celu kradzież danych. Ponadto sporo cyberprzestępców nie działa już jedynie na terytorium Rosji czy w obrębie Wspólnoty Niepodległych Państw, ale atakuje cele za granicą.

Więcej na temat ewolucji rosyjskojęzycznej cyberprzestępczości znajduje się na stronie https://r.kaspersky.pl/Kr4N7.

Japoński Chugoku Bank zabezpiecza nową aplikację mobilną z pomocą zestawu SDK firmy Kaspersky

22.10.2021 r. - W celu zapewnienia bezpieczeństwa danym i transakcjom w swojej nowej aplikacji bankowości mobilnej przeznaczonej dla klientów indywidualnych japoński bank Chugoku Bank Ltd. wykorzystał zestaw narzędzi do rozwoju oprogramowania Kaspersky Mobile Security SDK. Wychodząc naprzeciw potrzebom sektora finansowego, który wymaga wysoce bezpiecznych aplikacji oraz systemów do ochrony danych firmowych i klientów, rozwiązanie firmy Kaspersky nie tylko zapewnia należytą ochronę, ale również oferuje bogatą funkcjonalność oraz łatwość użytkowania.

Na skutek pandemii popularność bankowości mobilnej znacznie wzrosła w ciągu ostatnich 18 miesięcy[3]. Zamknięcie banków stacjonarnych oraz restrykcje nałożone na przemieszczanie się sprawiły, że coraz więcej klientów zaczęło korzystać z aplikacji w celu dokonania płatności, sprawdzenia salda czy przelania środków. Jednak wzrostowi liczby użytkowników towarzyszyła ewolucja taktyk stosowanych przez cyberprzestępców w celu

atakowania klientów oraz banków. W efekcie pojawiło się wiele nowych fałszywych aplikacji i trojanów oraz odnotowano więcej ataków z użyciem szkodliwego oprogramowania.

Kaspersky Mobile Security SDK to zestaw do rozwoju oprogramowania, który umożliwia łatwe dodanie funkcji bezpieczeństwa do aplikacji mobilnych. Chociaż jest stosowany na całym świecie, na rynku japońskim został wdrożony po raz pierwszy. Chugoku Bank postawił na rozwiązanie firmy Kaspersky głównie ze względu na oferowane przez nie zróżnicowane funkcje bezpieczeństwa, w tym zabezpieczenie przed phishingiem oraz fałszywymi aplikacjami, jak również funkcje wykrywania szkodliwego oprogramowania i ochrony danych. Bank wskazał również na wysoką opłacalność rozwiązania dzięki systemowi licencjonowania – główny wymóg w procedurze przetargowej.

Dzięki ścisłej współpracy między twórcami aplikacji bankowej a inżynierami z firmy Kaspersky wdrożenie usługi odbyło się sprawnie oraz bez opóźnień. Cały proces – od określenia wymogów po opracowanie i wydanie aplikacji – trwał jedynie sześć miesięcy.

Aplikacja banku umożliwia między innymi przeglądanie salda oraz szczegółów dotyczących konta, dokonywanie płatności

oraz przelewanie środków. W ciągu miesiąca od udostępnienia usługi (7 lipca 2021 r.) liczba użytkowników przekroczyła 20 000. Chugoku Bank planuje dalsze rozszerzenie funkcjonalności aplikacji oraz udoskonalenie usług.

[3] *https://www.techradar.com/news/mobile-banking-apps-could-be-major-security-threat-says-fbi*

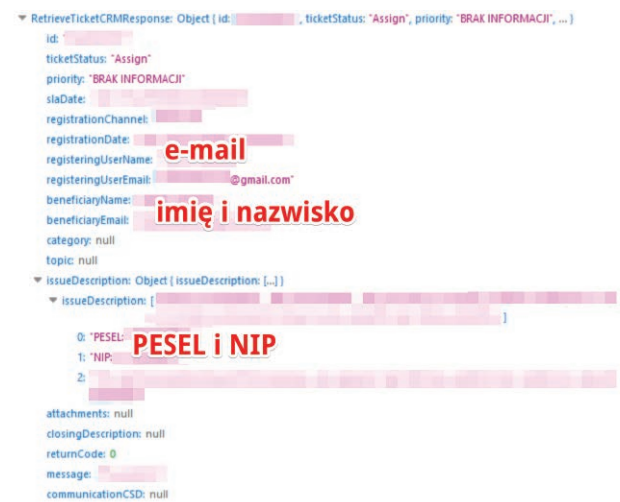
Dane użytkowników systemu e-TOLL można było sobie pobrać

26.10.2021 r. - Jak można przeczytać na łamach Niebezpiecznika, z systemu poboru opłat e-TOLL można było pobrać dane użytkowników, w tym ich numery PESEL. Winne okazało się niezbyt dobrze zabezpieczone API[4], które nie posiadało poprawnie zaimplementowanego uwierzytelniania użytkownika. Jeśli z zapytania usunęło się parametr beneficiaryId, po którym identyfikowany był aktualny użytkownik, można było zobaczyć obiekty z danymi ticketów, które zawierały informacje na temat innych użytkowników systemu, takie jak:

- imię i nazwisko,
- adres e-mail,
- numer telefonu,
- numer PESEL,
- numer NIP,
- szczegóły dotyczące przeglądarki i systemu operacyjnego użytkownika,
- saldo konta,
- historia wpłat i wypłat.

Ministerstwo Finansów potwierdziło usunięcie błędów i przesłało do redakcji Niebezpiecznika poniższe wyjaśnienia:

(...) System e-TOLL był audytowany pod kątem bezpieczeństwa przez podmiot zewnętrzny. Prace rozwojowe są realizowane punktowo, w II połowie października zostały zaplanowane kolejne zewnętrzne testy bezpieczeństwa, które mają zweryfikować aktualny stan bezpieczeństwa systemu. Obecnie prace skoncentrowane są nad usunięciem podatności, która mogła powstać 7.10.2021 w trakcie prac rozwojowych, m.in. związanych z uruchomieniem



formularza zgłoszeniowego na stronie WWW (regresja). Obecnie podatność związana obsługą ticketów została usunięta. MF dokonało analizy skutków wystąpienia tej podatności pod kątem naruszenia praw i wolności osób, których dane potencjalnie mogły być ujawnione. Na podstawie wyników tej analizy podjęto decyzję o zgłoszeniu naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, zgodnie z przepisami art. 33 Rozporządzenia PE i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Jednocześnie informujemy, że 15.10.2021 niezwłocznie, podjęliśmy analizę

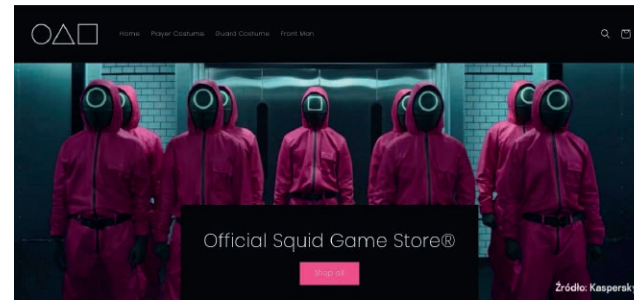
mającą na celu potwierdzenie istnienia zgłoszonej podatności dotyczącej nieautoryzowanego dostępu do ticketów. Po przeanalizowaniu skutków biznesowych podjęliśmy decyzję o wyłączeniu tej usługi. Użytkownik może nadal wykonywać zgłoszenia, otrzymuje informację (powiadomienie mailowe) o jego przekazaniu, natomiast na jego koncie po zalogowaniu nie są widoczne na chwilę obecną wykonane przez niego zgłoszenia. W efekcie wyłączenia usługi nie jest więc możliwe dalsze wykorzystywanie tej podatności. Zostały podjęte działania analityczne i developerskie, aby zabezpieczyć przed nieautoryzowanymi wywołaniami. Działania te będą prowadzone nieprzerwanie do momentu potwierdzenia jej usunięcia. Niezależnie od powyższych działań, zostały również podjęte prace mające na celu weryfikację, czy inne usługi nie mają podatności o podobnym charakterze. W przypadku zidentyfikowania podatności będą podejmowania działania skutkujące ich usunięciem.

W tym przypadku przyczyną dziury mogła okazać się pilna konieczność dopisania do systemu formularza zgłaszania błędów, który obsługiwał system ticketów. W sklepie Google Play można znaleźć wiele opinii, w których użytkownicy opisywanego systemu doświadczali z nim wiele problemów.

[4] *https://niebezpiecznik.pl/post/fatalna-wpadka-plusa-kazdy-mogl-pobrac-dane-klientow/*

Cyberprzestępcy wykorzystują popularność serialu Squid Game

kaspersky 27.10.2021 r. - W ciągu kilku miesięcy od premiery południowokoreański serial Squid Game stał się hitem Netfliksa, odnotowując ponad 111 milionów oglądających[5]. Naturalnie cyberprzestępcy nie zawahali się wykorzystać jego popularności, stosując dobrze znane oszustwa. Eksperci z firmy Kaspersky podsumowali swoje spostrzeżenia dotyczące najpowszechniejszych i najbardziej wyrafinowanych zagrożeń związanych z serialem, na jakie można trafić w internecie, łącznie z trojanami, oprogramowaniem adware oraz podejrzanymi ofertami kostiumów halloweenowych.



Przykład strony phishingowej, na której można rzekomo kupić gadżety związane z serialem Squid Game

Pobierz odcinek serialu Squid Game… a wraz z nim szkodliwe oprogramowanie

Od września do października 2021 r. badacze z firmy Kaspersky wykryli kilkadziesiąt różnych szkodliwych plików, których nazwy nawiązywały do serialu. W większości przeanalizowanych przypadków zidentyfikowano trojany pobierające inne szkodliwe programy, ale także oprogramowanie adware wyświetlające nachalne reklamy. Jedna z metod stosowanych przez cyberprzestępców wyglądała następująco: potencjalna ofiara jest kuszona możliwością rzekomego obejrzenia animowanej wersji pierwszej gry z serialu, a jednocześnie potajemnie uruchamiany jest trojan, który kradnie dane z różnych przeglądarek użytkowników i wysyła je do serwera cyberprzestępców. Ponadto, w jednym z folderów zostaje utworzony skrót, który może być wykorzystywany do uruchamiania trojana przy każdym kolejnym starcie systemu.

Badacze z firmy Kaspersky wykryli również mobilne szkodliwe oprogramowanie wykorzystujące popularność Squid Game. Chcąc pobrać odcinek serialu, użytkownik pobierał w rzeczywistości trojana. Po uruchomieniu się na urządzeniu szkodnik prosi serwer cyberprzestępczy o zadania do wykonania. Może to być np. otwarcie zakładki w przeglądarce lub wysłanie wiadomości SMS na numery wskazane przez atakujących. Trojan ten jest rozprzestrzeniany za pośrednictwem nieoficjalnych sklepów z aplikacjami oraz różnych portali, także pod przykrywką innych popularnych aplikacji, gier oraz książek.

Kup kostium z serialu Squid Game… i stracić pieniądze

Wraz ze zbliżającym się Halloween podstawowe pytanie brzmi: za jaką postać przebrać się w tym roku? Cyberprzestępcy i oszuści pomyśleli także o tym. Zaczyna pojawiać się wiele fałszywych sklepów nawiązujących do serialu Squid Game. Większość z nich oferuje możliwość zakupienia kostiumów noszonych przez graczy w serialu – takie sklepy przedstawiają się jako oficjalne. Jednak dokonując zakupów na stronach tego typu, użytkownicy najczęściej tracą pieniądze i nie otrzymają żadnego towaru. Co więcej, przekazują cyberprzestępcom informacje bankowe oraz osobowe, ponieważ są proszeni o podanie szczegółów dotyczących karty płatniczej, adresu e-mail, numeru telefonu, adresu zamieszkania czy imienia i nazwiska.

Przystąp do gry Squid Game online… i stracić swoje dane identyfikacyjne oraz bankowe

Badacze z firmy Kaspersky znaleźli także kilka stron, na których można rzekomo rywalizować w internetowej wersji gry Squid Game o główną wygraną – 100 BNB (Binance Coin). Nie trzeba dodawać, że gracz nie dostaje obiecanej nagrody i koniec końców traci swoje dane lub na jego urządzenie zostaje pobrane szkodliwe oprogramowanie.

[5] *https://www.euronews.com/culture/2021/10/13/squid-game-becomes-netflix-s-biggest-series-with-111-million-viewers-in-first-month*

Totolotek zhakowany

18.10.2021 r. - W październiku ubiegłego roku Totolotek został zainfekowany ransomwarem. O tym fakcie poinformował ofiary poprzez wiadomości e-mail. Zaszyfrowane zostały systemy, ale włamywacze mogli też ukraść dane użytkowników, takie jak: PESEL, nr dokumentu tożsamości, adres zamieszkania, adres e-mail, numer telefonu.

O sprawie poinformował Niebezpiecznik, który opublikował też pełną treść oświadczenia Totolotka:

Szanowna Pani / Szanowny Panie,

Prosimy o przeczytanie ważnej wiadomości.

Z ustaleń prowadzonego przez nas postępowania wyjaśniającego wynika, że w dniu 30 września 2021 r. Totolotek S.A. padł ofiarą przestępstwa (cyberataku). W rezultacie tego ataku, doszło do zaszyfrowania części archiwalnych danych, dotyczących okresu sprzed 22 lipca 2019 r. W chwili wykrycia nieprawidłowości nasze systemy IT zostały odłączone od sieci, celem zapobieżenia możliwości dostępu do danych Totolotek S.A. przez osoby nieuprawnione.

W ramach prowadzonego postępowania wyjaśniającego nie udało się wykluczyć możliwości, że osoby nieuprawnione mogły mieć dostęp do wskazanych poniżej danych. Kierując się troską o prywatność i bezpieczeństwo naszych klientów, przesyłamy więc niniejszą informację na temat danych, które mogły zostać ujawnione, możliwych konsekwencji ich ujawnienia oraz środków zaradczych, które można podjąć w celu zminimalizowania ryzyka z tym związanego.

Dane osobowe, do których dostęp mogły uzyskać osoby nieuprawnione, to dane archiwalne według stanu na dzień 21.07.2019 r. mogące obejmować: login, email, numer telefonu, imię, nazwisko, płeć, datę urodzenia, numer dowodu osobistego, PESEL, adres zamieszkania, numer rachunku bankowego.

W związku z tym, nie możemy wykluczyć, że Pani/Pana dane osobowe mogą być wykorzystane przez nieuprawnione osoby. Dane te mogą zostać użyte do (przykładowo) założenia konta w systemie informacji kredytowej, aby monitorować Pani/Pana aktywność kredytową, zaciągnięcia zobowiązań finansowych w instytucjach pozabankowych, założenia konta w serwisie społecznościowym, kierowania do Pani/Pana niezamówionych informacji handlowych drogą pocztową lub za pomocą poczty email. Jest nam bardzo przykro z powodu tego zdarzenia. Chcielibyśmy podkreślić, że podjęliśmy przewidziane prawem kroki i powiadomiliśmy o tym zdarzeniu właściwe instytucje – w tym organy ścigania oraz Urząd Ochrony Danych Osobowych. Podjęliśmy także niezbędne działania, aby podobne zdarzenie nie miało miejsca w przyszłości. Totolotek S.A. podjął już następujące kroki w celu ograniczenia ewentualnych skutków ataku, tj. serwery zostały permanentnie odcięte od internetu, trwa także proces informatyczny mający na celu utrudnienie oraz uniemożliwienie nieuprawnionego dostępu w przypadku prób przyszłych ataków. Ponadto, zachęcamy Państwa do rozważenia możliwości podjęcia następujących czynności, w celu zminimalizowania ryzyka związanego z ewentualnym wykorzystaniem Państwa danych przez osoby nieuprawnione: regularnego zmieniania haseł do Państwa konta, nieotwierania wiadomości od nieznanych nadawców, sprawdzenia Państwa historii kredytowej, zastrzeżenia kont w odniesieniu do których możliwe było uzyskanie dostępu na podstawie ww. danych, zastrzeżenie dowodu osobistego oraz natychmiastowe poinformowanie Policji, jeśli powezmą Państwo informacje, że jakiekolwiek z tych danych zostały wykorzystane przez osoby trzecie (...).

Jak zauważają redaktorzy Niebezpiecznika, w tym przypadku dane są kompletne i ułatwiają wyłudzenie pożyczki[6], kradzież tożsamości czy przejęcie konta w różnych systemach (także służących do generowania duplikatów kart SIM)[7].

[6] *https://niebezpiecznik.pl/post/oszustowi-do-wziecia-pozyczki-wystarczyly-publicznie-dostepne-dane/*

[7] *https://niebezpiecznik.pl/post/tmobile-duplikat-sim-swap/*

„Atak" z Loterią Narodowego Programu Szczepień w tle

5.11.2021 r. - W listopadzie 2021 roku jeden z czytelników serwisu niebezpiecznik.pl otrzymał taką wiadomość e-mail:

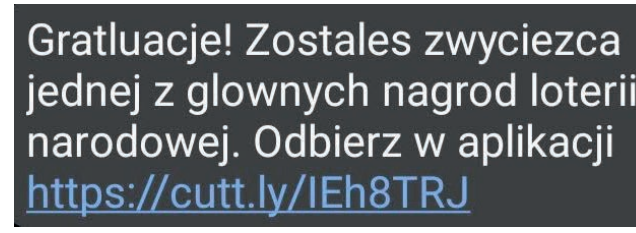
Witaj XXX,

Gratulujemy! Zostałeś jednym ze zwycięzców nagrody tygodniowej w loterii #SzczepimySię. Aby odebrać nagrodę musisz potwierdzić swoje dane, oraz wskazać adres dostawy.

Zweryfikuj swoje dane!

Dziękuję że dołączyłeś do zaszczepionych.

Adam Niedzielski, Minister Zdrowia



Wiadomość przyszła na firmowy adres e-mail i została zakwalifikowana jako spam po stronie odbiorcy. Zawarty w niej link prowadził do strony szczepimysie.org.pl, na której znajdował się jedynie formularz. Na oficjalnych stronach rządowych nie znajdowały się żadne informacje o domenie „szczepimysie.org.pl". Czytelnik, który zgłosił Niebezpiecznikowi tę sytuację, nie znalazł się też na oficjalnej liście zwycięzców https://www.gov.pl/web/loteria/tygodniowe/.

Zbieranie danych w zakresie PESEL i numer telefonu oraz adres — w kontekście weryfikacji zwycięzcy i odbioru nagrody — wydaje się być uzasadnione, jednak na rządowej stronie znajduje się informacja, że zwycięzcy otrzymują SMS-a z powiadomieniem o wygranej. A wspomniany czytelnik otrzymał wiadomość e-mail — i to na służbowy, niepodawany nigdzie w kontekście szczepienia adres.

Jeśli chodzi o domenę, wskazywała ona na adres IP: 94.152.11.118 (lexi.rev.domeny.host) i została zarejestrowana 2 lipca 2021 roku. Prawdopodobnie nie była ona wykorzystywana w masowych atakach. Redaktorzy Niebezpiecznika podejrzewają, że jest to jakaś infrastruktura, którą do ataków socjotechnicznych na swoich klientów wykorzystuje jakaś firma pentesterska.

Zamiast zastanawiać się, czy otrzymany SMS jest prawdziwy, wystarczy sprawdzić listę zwycięzców[8]. A wszelkie e-maile, w których ktoś prosi nas o podanie naszych danych osobowych i które trafiły do folderu ze spamem... zostawmy w spamie.

[8] *https://www.gov.pl/web/loteria/tygodniowe/*

W trzecim kwartale 2021 r. ataki DDoS odnotowały wzrost o 24% i stały się bardziej zaawansowane

8.11.2021 r. - W porównaniu z trzecim kwartałem 2020 r. łączna liczba ataków DDoS wzrosła o niemal 24%, z kolei całkowita liczba inteligentnych ataków (zaawansowanych, często ukierunkowanych, ataków DDoS) zwiększyła się o 31% w porównaniu z analogicznym okresem w biegłym roku. Wśród najbardziej znamiennych celów znalazły się narzędzia do walki z pandemią, organizacje rządowe, twórcy gier oraz znane publikacje poświęcone cyberbezpieczeństwu.

Ataki DDoS (ang. *Distributed Denial of Service*) przeprowadza się w celu przeciążenia serwera sieciowego sztucznymi żądaniami, aby doprowadzić do awarii usługi lub jej całkowitego zatrzymania. Może to spowodować ogromne zakłócenia w organizacjach i biznesie, ponieważ tego rodzaju ataki mogą trwać od kilku minut do kilku dni. Tak zwane „inteligentne" ataki DDoS posuwają się o krok dalej: są bardziej wyrafinowane i często również wymierzone w określone cele. Ponadto mogą być wykorzystane nie tylko do zakłócenia usług, ale również uniemożliwienia dostępu do pewnych zasobów lub kradzieży pieniędzy. Oba rodzaje ataków odnotowały wzrost w III kwartale 2021 r.

W porównaniu z III kwartałem ubiegłego roku łączna liczba ataków DDoS zwiększyła się o niemal 24%, z kolei całkowita liczba „inteligentnych" ataków wzrosła o 31%. Oba rodzaje ataków odnotowały również wzrost w stosunku do II kwartału 2021 r., przy czym największy odsetek zaatakowanych zasobów (40,8%) znajdował się w Stanach Zjednoczonych, następnie w Hongkongu oraz w Chinach kontynentalnych. W sierpniu badacze z firmy Kaspersky odnotowali rekordową liczbę ataków DDoS w ciągu jednego dnia: 8 825.

W minionym kwartale jedne z najistotniejszych, przeprowadzonych na dużą skalę ataków DDoS wykorzystywały nowy, potężny botnet o nazwie Mēris, który potrafi wysyłać ogromną liczbę żądań na sekundę. Botnet ten został zidentyfikowany w atakach na dwie z najbardziej znanych publikacji poświęconych cyberbezpieczeństwu – Krebs on Security oraz InfoSecurity Magazine.

Wśród innych istotnych trendów w zakresie ataków DDoS w III kwartale można wyróżnić: serię motywowanych względami politycznymi ataków w Europie oraz Azji, jak również ataki na twórców gier. Ponadto cyberprzestępcy brali na celownik zasoby służące do walki z pandemią w kilku krajach. Miała także miejsce seria ataków ransomware wymierzonych w dostawców usług telekomunikacyjnych w Kanadzie, Stanach Zjednoczonych oraz Wielkiej Brytanii. Atakujący przedstawili się jako członkowie niesławnego ugrupowania ransomware o nazwie REvil i wyłączyli serwery atakowanych firm w celu wymuszenia na nich zapłaty okupu.

Badacze z firmy Kaspersky zaobserwowali również wysoce nietypowy, trwający kilka dni atak na jednym z uniwersytetów państwowych. Chociaż ataki na zasoby edukacyjne nie są rzadkością, ten konkretny przypadek odznaczał się wyjątkowym stopniem wyrafinowania. Celem ataku były konta online kandydatów ubiegających się o przyjęcie na uniwersytet, a cyberprzestępcy wybrali wektor ataków, który spowodował całkowitą niedostępność zasobu. Ponadto – co zdarza się rzadko – atak był kontynuowany nawet po rozpoczęciu filtrowania sztucznego ruchu.

Więcej informacji na temat ewolucji ataków DDoS w III kwartale 2021 r. znajduje się na stronie https://r.kaspersky.pl/lWRTW.

Media Markt i Saturn zhackowane

8.11.2021 r. - W listopadzie ubiegłego roku sieć i serwery grupy Media Markt i Saturn zostały zaatakowane, a część z nich została zaszyfrowana. Atak dotknął całą Europę, a Media Markt otrzymał żądanie okupu — 240 milionów dolarów. Ostatecznie firmie udało się znegocjować okup do 50 milionów dolarów.

Ransomware, które zaatakowało firmę, to najprawdopodobniej Hive. Grupa jest aktywna od połowy 2021 roku i ma na swoim koncie kilkadziesiąt ofiar, w tym szpitale. Jego celem są zwykle maszyny działające pod kontrolą systemu Linux.

Niebezpiecznik opublikował komentarz polskiego oddziału Media Markt:

MediaMarktSaturn Retail Group stał się celem działań o charakterze cyber-przestępczym. Firma natychmiast zawiadomiła

odpowiednie władze i pracuje intensywnie, aby zidentyfikować systemy, których dotyczy problem i jak najszybciej naprawić poniesione szkody. W sklepach stacjonarnych dostęp do niektórych usług może być obecnie ograniczony. MediaMarktSaturn intensywnie pracuje nad tym, aby wszystkie usługi jak najszybciej były ponownie dostępne bez ograniczeń. Firma będzie informowała o dalszych działaniach.

Luxmed informuje o incydencie

9.11.2021 r. - Centrum Medyczne Luxmed z Lublina poinformowało o „usterce", która powodowała „otwarty dostęp" do danych osobowych pacjentów w zakresie: numeru PESEL, imię i nazwisko, adres e-mail, zaszyfrowane hasło do e-rezerwacji.

Wedle firmy „wycieku danych nie stwierdzono". Poniżej pełne oświadczenie, jakie Centrum Medyczne Luxmed przesłało swoim klientom:

Szanowni Państwo,

Informujemy, że w naszej strukturze informatycznej znaleźliśmy usterkę, która spowodowała otwarty dostęp do Państwa danych, takich jak : imię, nazwisko, numery PESEL, adres e-mail, zaszyfrowane hasło do e-rezerwacji.

Dostęp został natychmiast zablokowany, a defekt naprawiony. Rozpoczęliśmy procedurę zgłaszania incydentu bezpieczeństwa do Urzędu Ochrony Danych Osobowych.

Nie stwierdziliśmy faktycznego wycieku danych, jedynie błąd systemu, który mógłby taki wyciek spowodować.

Hasła zapisane były w postaci zaszyfrowanej, nie mniej jednak rekomendujemy zmianę hasła do Państwa konta w e-rezerwacji. Państwa hasło zostało przez nas zablokowane. Jeżeli to samo hasło jest używane do Państwa skrzynki pocztowej to ze względów bezpieczeństwa również rekomendujemy jego zmianę.

(...)

Podobno pracowników poinformowano o ataku już przed otwarciem sklepów, czyli o 8:30. Dane na komputerach pracowników nie zostały zaszyfrowane, ale ucierpiało wszystko, co jest na serwerach (systemy sprzedaży, kontroli, ustalania cen, przyjęcia towaru, fakturowania).

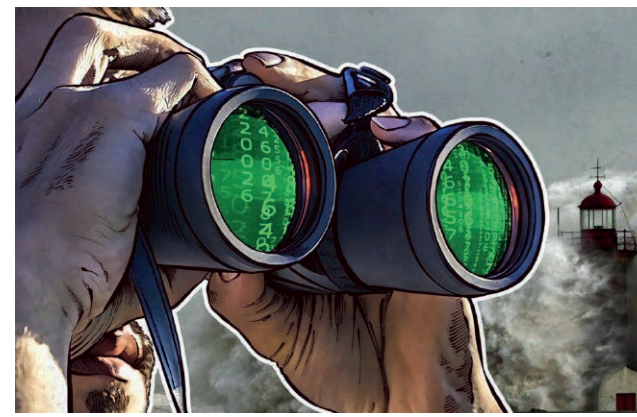
Sprzedaż stacjonarna odbywała się prawie normalnie — prawie, bo pracownik bez dostępu do swoich systemów nie jest w stanie na przykład sprawdzić, czy w sklepie jest konkretny towar. Z kolei odbiór zamówień internetowych był niemożliwy — ze względu na atak personel nie mógł oznaczyć, że konkretny sprzęt został odebrany przez klienta.

Zaawansowane cyberataki w 2022 r.: czego należy spodziewać się w przyszłym roku

17.11.2021 r. - Badacze z firmy Kaspersky zaprezentowali swoją wizję najbliższej przyszłości w zakresie zaawansowanych cyberataków, wskazując, jak zmieni się krajobraz zagrożeń w 2022 r. Odgrywające coraz większą rolę w cyberprzestrzeni upolitycznienie, powrót ataków uderzających jeszcze przed startem systemu operacyjnego, przypływ nowych ugrupowań APT oraz wzrost liczby ataków na łańcuch dostaw to niektóre z prognoz badaczy.

Zmiany, jakie zaszły na świecie w 2021 r., będą miały bezpośredni wpływ na rozwój zaawansowanych ataków w przyszłym roku. Na podstawie trendów zaobserwowanych przez Globalny Zespół ds. Badań i Analiz (GReAT) firmy Kaspersky w 2021 r. badacze stworzyli prognozę, która pomoże środowisku IT przygotować się na stojące przed nim wyzwania.

W tym roku w centrum uwagi znalazło się wykorzystywanie oprogramowania do monitoringu tworzonego przez prywatnych twórców. Odpowiadał za to Pegasus, który zmienił postrzeganie prawdopodobieństwa rzeczywistych ataków dnia zerowego na system iOS. Ponadto twórcy zaawansowanych narzędzi do monitoringu udoskonalili swoje możliwości unikania wykrycia oraz uniemożliwiania analizy – czego przykładem jest FinSpy – jak również wykorzystywania tych narzędzi w rzeczywistych warunkach.



Potencjał komercyjnego oprogramowania do monitoringu – m.in. dostęp do ogromnych ilości danych osobowych i szerszej puli celów – sprawia, że stanowi ono lukratywny biznes dla tych, którzy je dostarczają, i skuteczne narzędzie w rękach cyberprzestępców. Dlatego zdaniem ekspertów z firmy Kaspersky dostawcy takiego oprogramowania rozpoczną ekspansję w cyberprzestrzeni i będą świadczyć swoje usługi nowym, zaawansowanym ugrupowaniom cyberprzestępczym, dopóki rządy nie zaczną

regulować stosowanie narzędzi tego typu.

Pozostałe prognozy dotyczące zaawansowanych cyberzagrożeń w 2022 r.:

- **Urządzenia mobilne będą celem wyrafinowanych ataków przeprowadzanych na szeroką skalę.** Urządzenia mobile zawsze stanowiły łakomy kąsek dla cyberprzestępców – w końcu smartfony towarzyszą swoim właścicielom wszędzie i każdy z nich stanowi potencjalny cel oferujący ogromne ilości cennych informacji. W 2021 r. odnotowano więcej ataków dnia zerowego na system iOS w rzeczywistych warunkach niż kiedykolwiek wcześniej. W przeciwieństwie do komputerów PC lub Maców, na których użytkownik może zainstalować pakiet bezpieczeństwa, w przypadku systemu iOS tego rodzaju produkty są ograniczone lub po prostu nie istnieją. To stwarza wyjątkowe możliwości ugrupowaniom cyberprzestępczym.
- **Wzrost liczby ataków na łańcuch dostaw.** Badacze z firmy Kaspersky zwrócili szczególną uwagę na częstotliwość przypadków wykorzystania przez cyberprzestępców słabych punktów w zabezpieczeniach dostawców w celu infekowania urządzeń firm będących ich klientami. Tego rodzaju ataki są szczególnie lukratywne i wartościowe dla cyberprzestępców, ponieważ zapewniają dostęp do ogromnej liczby potencjalnych celów. Z tego powodu przewiduje się tendencję wzrostową ataków na łańcuch dostaw w 2022 r.
- **Cyberprzestępcy nadal będą wykorzystywali pracę zdalną.** Atakujący będą kontynuowali wykorzystywanie niezabezpieczonych lub niezałatanych komputerów osób pracujących zdalnie w celu przeniknięcia do sieci korporacyjnych. Nadal będziemy obserwować socjotechnikę stosowaną w celu kradzieży danych uwierzytelniających oraz ataki siłowe na serwisy korporacyjne w celu uzyskania dostępu do słabo chronionych serwerów.
- **Eksplozja ataków na zabezpieczenia chmury i usługi zlecane na zewnątrz.** Wiele firm wdraża przetwarzanie w chmurze oraz architektury oprogramowania oparte na mikrousługach i działające na infrastrukturze zewnętrznej, które są bardziej podatne na ataki cyberprzestępców. Tym samym coraz więcej firm będzie stanowiło w przyszłym roku główne cele wyrafinowanych ataków.
- **Powrót ataków niskiego poziomu: bootkity w akcji.** Ze względu na rosnącą popularność funkcji pozwalających na bezpieczny rozruch systemu operacyjnego (Secure Boot) cyberprzestępcy zmuszeni są szukać exploitów lub nowych luk w tym mechanizmie w celu obejścia jego systemu bezpieczeństwa. Dlatego badacze z firmy Kaspersky spodziewają się w 2022 r. wzrostu liczby bootkitów, które aktywowane są jeszcze przed startem systemu operacyjnego.
- **Państwa jasno zdefiniują dopuszczalne praktyki w zakresie cyberataków.** Badacze z firmy Kaspersky obserwują coraz większą tendencję wśród rządów, by zarówno potępiać wymierzone w nie cyberataki, jak i przeprowadzać własne w ramach kontrofensywy. W przyszłym roku niektóre państwa opublikują własną taksonomię cyberataków, wyróżniając akceptowalne rodzaje działań tego typu.

Prognozy dotyczące zaawansowanych cyberataków zostały przygotowane dzięki usługom analizy zagrożeń firmy Kaspersky stosowanym na całym świecie. Pełny raport jest dostępny na stronie https://r.kaspersky.pl/sDBsG. Dodatkowo 17 listopada o godz. 15:00 eksperci z zespołu GReAT firmy Kaspersky poprowadzą webinarium, podczas którego będą rozmawiali na temat przewidywanych zmian dot. głównych ugrupowań cyberprzestępczych w 2022 r. oraz dokonają oceny 2021 r. Udział w sesji jest bezpłatny i wymaga jedynie rejestracji na stronie https://kas.pr/91bh.

Czarny Piątek: ponad trzykrotnie więcej cyberataków związanych z płatnościami online

22.11.2021 r. - W okresie poprzedzającym wyprzedaże z okazji Czarnego Piątku odnotowano wzrost liczby ataków phishingowych podszywających się pod strony płatności elektronicznych. Według raportu[9] badaczy z firmy Kaspersky łączna liczba ataków wycelowanych w osoby korzystające z e-płatności zwiększyła się ponad trzykrotnie w okresie od września do października 2021 r.

Z nadejściem sezonu wyprzedaży ręce zacierają zarówno klienci, jak i sprzedawcy. Niestety jest to także ulubiony okres cyberprzestępców, którzy bez skrupułów zarabiają na klientach online poprzez tworzenie fałszywych stron podszywających się pod największe platformy handlowe oraz systemy e-płatności.

W pierwszych dziesięciu miesiącach 2021 r. produkty firmy Kaspersky wykryły ponad 40 milionów ataków phishingowych na platformy e-handlu oraz sklepy elektroniczne, jak również instytucje bankowe. Chociaż w 2021 r. sytuacja sklepów wróciła do normy, a klienci wrócili do zakupów stacjonarnych, badacze z firmy Kaspersky nie zaobserwowali typowych sezonowych trendów w phishingu związanych z zakupami online, takich jak znaczący przyrost liczby stron phishingowych z kuszącymi ofertami sprzedaży czy wzrost liczby oszustw związanych z handlem.

Istnieje jeden istotny wyjątek. W 2021 roku łączna liczba prób phishingu finansowego, których celem były systemy e-płatności, wzrosła ponad trzykrotnie od września (627 560) do października (1 935 905). Wzrosła również liczba wiadomości spamowych wykrytych przez produkty firmy Kaspersky. W ciągu miesiąca w okresie wyprzedaży, od 27 października do 19 listopada, zaobserwowano aktywne rozprzestrzenianie się wiadomości spamowych, z których 221 745 zawierało słowa „Black Friday".

Badacze z firmy Kaspersky sprawdzili również, które popularne platformy były wykorzystywane jako przynęta w rozprzestrzenianiu stron phishingowych. Najpopularniejszym wabikiem okazał się Amazon, o czym świadczyła łączna liczba prób phishingowych wykorzystujących tę nazwę. Przez większość 2021 r. drugą pod względem popularności przynętą był eBay, a następnie Alibaba.

Więcej informacji związanych z zagrożeniami i oszustwami wykorzystującymi popularność Czarnego Piątku znajduje się na stronie https://r.kaspersky.pl/vvKmA.

[9] *https://securelist.com/black-friday-2021/104915/*

Cyberzagrożenia finansowe w 2022 r.: systemy e-płatności i kryptowaluty na celowniku

kaspersky

23.11.2021 r. - Według badaczy z firmy Kaspersky w nadchodzącym roku ugrupowania cyberprzestępcze będą intensywnie atakować branżę kryptowaluty, a także żerować na inwestorach poprzez tworzenie fałszywych portfeli zawierających tylne furtki. Ponadto zaobserwujemy wzrost liczby ataków na systemy e-płatności, więcej trojanów kradnących informacje oraz bardziej zaawansowane zagrożenia mobilne.

Rok 2021 był okresem wyzwań i nowości, a cyberprzestępcy zawsze szybko adaptują się i nawigują wśród zmian na swoją korzyść. Ponieważ pieniądze są dla większości z nich głównym czynnikiem motywującym, zagrożenia finansowe zawsze stanowiły jeden z najistotniejszych elementów krajobrazu zagrożeń. Zastanawiając się nad istotnymi wydarzeniami i trendami, które ukształtowały sektor zagrożeń finansowych w 2021 r., badacze z firmy Kaspersky nakreślili kilka istotnych trendów, których spodziewają się w 2022 r.

- **Wzrost liczby ataków wycelowanych w kryptowalutę.** Kryptowaluta jest zasobem cyfrowym, wszystkie transakcje odbywają się online, a w dodatku oferuje ona użytkownikom anonimowość. Wszystko to jest atrakcyjne dla ugrupowań cyberprzestępczych. Jednak branżę tę atakują nie tylko organizacje cyberprzestępcze, ale również ugrupowania sponsorowane przez rządy. Badacze z firmy Kaspersky zaobserwowali już pojawienie się cybergangów agresywnie atakujących biznes kryptowalutowy i spodziewają się zwiększenia intensywności tych działań.
- **Fałszywe portfele sprzętowe i socjotechnika zagrożeniem dla inwestorów.** Podczas gdy ataki na walutę cyfrową stają się coraz precyzyjniejsze, cyberprzestępcy nieustannie wymyślają nowe sposoby kradzieży zasobów finansowych inwestorów. W kontekście inwestowania w kryptowalutę badacze z firmy Kaspersky przewidują, że cyberprzestępcy będą rozwijać i sprzedawać fałszywe urządzenia z tylnymi furtkami oraz stosować kampanie socjotechniczne i inne techniki w celu kradzieży zasobów finansowych ofiar.
- **Wzrost liczby trojanów kradnących informacje.** Czynniki takie jak prostota, przystępność oraz skuteczność ataków odegrają kluczową rolę w zaadaptowaniu szkodliwego oprogramowania kradnącego dane do ataków na zasoby finansowe — przynajmniej jako modułów zbierających dane w pierwszej fazie ataku. Ugrupowania cyberprzestępcze wykorzystają takie podejście do profilowania ofiar celem przeprowadzenia dalszych szkodliwych działań. Dotyczy to między innymi precyzyjnych ataków ransomware.
- **Rozwój cyberzagrożeń mobilnych.** Pandemia przyspieszyła rozwój bankowości mobilnej, która osiągnęła również większą dojrzałość. Eksperci z firmy Kaspersky spodziewają się większej liczby mobilnych trojanów bankowych dla platformy Android, w szczególności narzędzi zdalnej administracji, które mogą obejść środki bezpieczeństwa stosowane przez banki. Lokalne i egionalne projekty cyberprzestępcze dotyczące szkodników dla Androida osiągną skalę globalną, eksportując ataki do Europy Zachodniej i reszty świata.

Więcej informacji na temat pr ognoz związanych z cyberprzestępczością wycelowaną w sektor finansowy znajduje się na stronie https://r.kaspersky.pl/Re4EZ.

Porady z okazji Międzynarodowego Dnia Bezpieczeństwa Komputerowego

kaspersky

30.11.2021 r. - 30 listopada obchodzimy Międzynarodowy Dzień Bezpieczeństwa Komputerowego. Z tej okazji eksperci z firmy Kaspersky przypominają kilka podstawowych faktów i zasad cyberbezpieczeństwa, które pozwolą zadbać o należytą ochronę urządzeń i życia cyfrowego.

Od lipca do września 2021 r. rozwiązania firmy Kaspersky:

- Zablokowały 1,1 mld ataków z zasobów online na całym świecie.
- Zidentyfikowały 35,9 mln szkodliwych programów.
- Powstrzymały próby uruchomienia szkodliwego oprogramowania w celu kradzieży pieniędzy z kont bankowych online na komputerach 104 257 unikatowych użytkowników.

- Zablokowały 46,3 mln prób otworzenia odsyłaczy phishingowych prowadzących do sfałszowanych stron mających na celu wyłudzanie danych.

Jak najlepiej uczcić Międzynarodowy Dzień Bezpieczeństwa Komputerowego? Zastanawiając się nad bezpieczeństwem swojego komputera, danych sieciowych oraz magazynu w chmurze. Można z tej okazji np. zmienić swoje hasło, włączyć uwierzytelnienie dwuskładnikowe lub po prostu wpisać w wyszukiwarce Google swoje imię i nazwisko, by sprawdzić, jakie dane na nasz temat są dostępne publicznie.

Eksperci z firmy Kaspersky przygotowali krótki poradnik, dzięki któremu można łatwo wzmocnić bezpieczeństwo komputerowego oraz zadbać o prywatność w przestrzeni cyfrowej. Specjaliści zalecają wykonanie następujących działań:

- Przeprowadź aktualizację oprogramowania na wszystkich urządzeniach. Wiele problemów z bezpieczeństwem można rozwiązać, instalując uaktualnione wersje oprogramowania. Według badania[10] przeprowadzonego niedawno przez firmę Kaspersky 50% użytkowników, po otrzymaniu powiadomienia o aktualizacji, klika przycisk „przypomnij mi później", ponieważ są zajęci innymi sprawami. Takie podejście może się zemścić, ponieważ uaktualnienia często usuwają błędy w zabezpieczeniach, które mogą zostać wykorzystane przez cyberprzestępców.
- Zainstaluj solidne i godne zaufania rozwiązanie bezpieczeństwa i postępuj zgodnie z jego zaleceniami. Dobry pakiet bezpieczeństwa rozwiąże większość problemów automatycznie i w razie potrzeby powiadomi Cię o konieczności wykonania pewnych działań.
- Zadbaj o hasła. Warto regularnie aktualizować podstawowe hasła do poczty, platform społecznościowych oraz innych usług online. Najważniejsza zasada brzmi jednak: nie używaj tego samego hasła do wielu kont. Aby sprawdzić, jak bezpieczne jest Twoje hasło, wejdź na stronę: https://password.kaspersky.com/pl. W przypadku problemów z zapamiętaniem wszystkich haseł możesz skorzystać z niezawodnego menedżera haseł, który nie tylko pozwoli przechowywać wszystkie hasła w jednym miejscu, ale również pomoże wygenerować nowe, silne hasła.
- Włącz uwierzytelnienie dwuskładnikowe. Czekanie na kod w SMS-ie, gdy szybko chcesz otworzyć określony zasób online, może na pierwszy rzut oka wydawać się stratą czasu. Jednak uwierzytelnienie dwuskładnikowe jest jednym z najskuteczniejszych narzędzi zapobiegających hakowaniu konta oraz kradzieży tożsamości online.
- Sprawdzaj uprawnienia przyznane aplikacjom mobilnym oraz rozszerzeniom przeglądarek.
- Regularnie twórz kopię zapasową ważnych danych. Bezpieczną opcją jest wykonanie dwóch kopii: jednej przechowywanej w chmurze, a drugiej na fizycznym nośniku (takim jak przenośny dysk twardy, karta pamięci, pendrive itd.), który nie jest na stałe podłączony do komputera. Od czasu do czasu sprawdź, czy kopia zapasowa jest sprawna.

Więcej porad bezpieczeństwa można znaleźć na oficjalnym blogu firmy Kaspersky – Kaspersky Daily: https://kaspersky.pl/blog.

[10] *https://media.kasperskydaily.com/wp-content/uploads/sites/92/2021/06/09104502/7919_B2B_2020_Report_A4_v3_WEB1.pdf*

Kaspersky opracowuje zasady cyberbezpieczeństwa urządzeń bionicznych

1.12.2021 r. - Firma Kaspersky jest jedną z pierwszych organizacji, która odniosła się do zjawiska doskonalenia organizmu ludzkiego (ang. human augmentation), prezentując wszechstronne zasady cyberbezpieczeństwa w tym kontekście. Celem dokumentu jest zwiększenie możliwości pracowników przy jednoczesnym uwzględnieniu ich bezpieczeństwa podczas wykorzystywania urządzeń bionicznych w biurze.

Koncepcję doskonalenia organizmu ludzkiego otacza atmosfera ekscytacji oraz innowacji – szczególnie w odniesieniu do coraz częstszego wykorzystywania urządzeń bionicznych w celu zastąpienia lub udoskonalenia części ciała przy użyciu sztucznych implantów – w której przebijają jednak pewne obawy ekspertów oraz szerszej społeczności. Powodem ich niepokoju jest zbyt mała uwaga poświęcana bezpieczeństwu takich specjalistycznych urządzeń. Brak świadomości związanej z tym tematem jest źródłem niepewności oraz zagrożeń zarówno dla dalszego rozwoju technologii doskonalenia organizmu ludzkiego, jak i bezpieczniejszego świata cyfrowego w przyszłości.

Firma Kaspersky nieprzerwanie bada potencjał doskonalenia organizmu człowieka oraz ocenia wyzwania dla bezpieczeństwa, wobec których być może staniemy, jeśli taka technologia zostanie zintegrowana z naszym życiem na szerszą skalę. W efekcie otwartych dyskusji prowadzonych w społeczności firma Kaspersky postanowiła odpowiedzieć na potrzebę regulacji bezpieczeństwa i stworzyła zasady cyberbezpieczeństwa mające na celu złagodzenie zagrożeń, jakie technologia doskonalenia organizmu człowieka może stwarzać dla korporacyjnych sieci IT. Dokument[11] zawiera scenariusz, który przewiduje, że pracownicy „udoskonaleni" za pomocą takiej technologii będą w przyszłości częściej spotykani w firmach, i uwzględnia rzeczywiste testy[12] firmy Kaspersky obejmujące biochipy.

Nowe zasady bezpieczeństwa określają procedury wykorzystywania urządzeń bionicznych[13] w firmie i mają na celu zmniejszenie zagrożeń dla cyberbezpieczeństwa w procesach biznesowych. Zaproponowany dokument dotyczy infrastruktury całej firmy i wszystkich jej jednostek biznesowych. Ma zatem zastosowanie do systemu kontroli dostępu, jak również procesów administracyjnych, procesów utrzymania oraz wykorzystywania systemów zautomatyzowanych. Zaproponowany zestaw zasad

obejmuje zarówno osoby zatrudnione, personel tymczasowy, jak i pracowników interesariuszy zewnętrznych świadczących wobec firmy usługi na mocy kontraktu. Wszystkie te czynniki mają na celu zwiększenie cyberbezpieczeństwa infrastruktury korporacyjnej.

Zaproponowana przez firmę Kaspersky polityka cyberbezpieczeństwa oferuje szereg procesów standaryzacji, które wzmacniają ochronę i zapewniają większą inkluzywność pracowników wykorzystujących urządzenia bioniczne w biurze. Jednym z głównych celów tej inicjatywy jest również włączenie globalnej społeczności IT oraz związanej z technologią human augmentation do dyskusji oraz zachęcenie do prowadzenia wspólnych działań w kierunku dalszego rozwoju bezpieczeństwa doskonalenia organizmu ludzkiego. Dotyczy to zapewnienia cyfrowej prywatności urządzeń, przyznania różnych poziomów praw dostępu do zgromadzonych informacji oraz łagodzenia wszelkich zagrożeń związanych ze zdrowiem ludzkim.

Kolejna międzynarodowa dyskusja na temat przyszłości doskonalenia organizmu ludzkiego, globalnej polityki przemysłowej, standardów bezpieczeństwa cyfrowego, największych zagrożeń cyfrowych, które mogą być związane z technologiami doskonalenia organizmu ludzkiego, jak również najlepszych praktyk dot. ich zwalczania, odbędzie się 7 grudnia 2021 r. podczas Szczytu Cyfrowego ONZ 2021[14].

Więcej informacji oraz możliwość rejestracji na dyskusję panelową online, która odbędzie się 7 grudnia 2021 r. w ramach Szczytu Cyfrowego ONZ 2021, znajduje się na stronie https://www.intgovforum.org/en/content/igf-2021-town-hall-32-the-future-of-human-augmentation-gain-or-cyber-pain.

[11] *https://media.kasperskydaily.com/wp-content/uploads/sites/90/2021/11/26201232/Security-policy-for-bionic-devices-EN-final.pdf*

[12] *https://plblog.kaspersky.com/?s=bionic+man+diary*

[13] *Urządzenia bioniczne, o których mowa w zasadach cyberbezpieczeństwa, obejmują elektroniczne chipy (takie jak np. biochip NFC), bioniczne protezy kończyn oraz organy wewnętrzne, jak również sztuczne organy sensoryczne (np. protezy wzrokowe, aparaty słuchowe itd.).*

[14] *https://www.intgovforum.org/en/content/igf-2021-town-hall-32-the-future-of-human-augmentation-gain-or-cyber-pain*

Kaspersky podzielił się swoją cyberwiedzą oraz poprowadził debaty podczas Szczytu Cyfrowego ONZ 2021

3.12.2021 r. - Drugi rok z rzędu firma Kaspersky wzięła udział w Szczycie Cyfrowym ONZ, którego gospodarzem była tym razem Polska. Podczas szczytu, który odbył się w formie hybrydowej w Katowicach w dniach 6-10 grudnia 2021 r., eksperci z firmy Kaspersky mieli okazję przyczynić się do tworzenia intensywnego globalnego dialogu dotyczącego zaufania, bezpieczeństwa, stabilności oraz inkluzywnego zarządzania internetem.

XXVI Szczyt Cyfrowy ONZ IGF[15] był platformą dla ponad 250 profesjonalnych sesji, w których wzięło udział ponad 1 000 prelegentów z ponad 175 krajów. Konferencja zgromadziła różne grupy interesariuszy pod głównym hasłem „Zjednoczony internet".

Ostatni rok wyraźnie pokazał, że ewoluujący globalny cyberkrajobraz oraz coraz większa zależność ludzi, organizacji, łańcuchów dostaw oraz infrastruktury krytycznej od internetu stanowią nowe zagrożenia nie tylko dla firm prywatnych, ale również całych branż, a nawet gospodarek narodowych. Obecny cyberkontekst podkreśla potrzebę międzynarodowej współpracy rozmaitych zainteresowanych stron w celu lepszego zrozumienia, w jaki sposób można zmaksymalizować możliwości, jakie daje internet, przeciwdziałać zagrożeniom i zrozumieć wyłaniające się wyzwania.

W tym roku firma Kaspersky miała zaszczyt zorganizować w ramach konferencji kilka sesji oraz interaktywnych warsztatów, podczas których przedstawiła rozwój globalnego cyberkrajobrazu w celu wzmocnienia międzynarodowej współpracy dotyczącej cyberbezpieczeństwa oraz cyberodporności. Tematami dyskusji były między innymi, zmieniające się wyzwania łańcuchów dostaw, ochrona infrastruktury krytycznej, rozwój technologii doskonalenia organizmu ludzkiego oraz rosnąca potrzeba globalnej policji cyberbezpieczeństwa.

[15] *https://www.intgovforum.org/en/dashboard/igf-2021*

Niemal połowa incydentów naruszenia bezpieczeństwa badanych w 2021 r. przez firmę Kaspersky była powiązana z ransomware

7.12.2021 r. - O reagowaniu na incydent mówimy, gdy ma miejsce zdarzenie związane z naruszeniem bezpieczeństwa i firmy wzywają zespół specjalistów w celu ograniczenia szkód lub zapobiegnięcia rozprzestrzenianiu się ataku. W firmie Kaspersky reagowanie na incydenty jest zarezerwowane dla średnich i dużych firm i zajmuje się nim specjalny dział – Global Response Emergency Team (GERT). Od stycznia do listopada 2021 r. niemal co drugi incydent obsługiwany przez zespół GERT był powiązany z oprogramowaniem ransomware (prawie 50% wszystkich zgłoszeń) – co stanowi wzrost o niemal 12% w porównaniu z 2020 r.

Jeśli chodzi o cyberbezpieczeństwo, oprogramowanie ransomware stało się w tym roku niekwestionowanym „bohaterem" nagłówków medialnych. Operatorzy ransomware udoskonalili swój arsenał, koncentrując się na mniejszej liczbie ataków na duże organizacje. Powstał nawet cały podziemny ekosystem wspierający działania cybergangów.

W pierwszych jedenastu miesiącach bieżącego roku odsetek incydentów związanych z ransomware, którymi zajmował się zespół GERT firmy Kaspersky, stanowił 46,7% wszystkich obsługiwanych zdarzeń (dla porównania: w 2020 i 2019 r. stanowił odpowiednio 37,9% i 34%). Najczęstsze cele tego rodzaju ataków stanowił sektor rządowy i przemysłowy. Łącznie ataki na te dwa sektory odpowiadały w 2021 r. za niemal połowę wszystkich zgłoszeń związanych z oprogramowaniem ransomware. Inne popularne cele obejmowały instytucje IT oraz finansowe.

Jednak gdy operatorzy ransomware zaczęli żądać wyższych okupów oraz atakować znane cele, spotkali się z rosnącą presją ze strony polityków oraz organów ścigania – co zmusiło ich do zwiększenia skuteczności ataków. W efekcie eksperci z firmy Kaspersky zaobserwowali dwa istotne trendy, które zyskają na popularności w nadchodzącym roku. Po pierwsze, gangi ransomware będą prawdopodobnie częściej tworzyły linuksowe kompilacje ransomware w celu zmaksymalizowania powierzchni ataków. Miało to już miejsce w przypadku takich ugrupowań jak RansomExx czy DarkSide. Ponadto operatorzy ransomware zaczną koncentrować się w większym stopniu na „szantażu finansowym[16]". Ma on miejsce wtedy, gdy operatorzy ransomware grożą ujawnieniem informacji na temat firm, które są w trakcie krytycznych procesów finansowych (np. dokonywanie fuzji lub przejęcia, planowanie wejścia na giełdę), w celu zaniżenia wartości ich udziałów. Firmy, które znajdują się w tak wrażliwej sytuacji finansowej, są bardziej skłonne zapłacić okup.

Dalsze informacje dotyczące ataków ransomware w 2021 r. i prognoz na nadchodzący rok są dostępne na stronie https://r.kaspersky.pl/Tc6p2.

[16] *https://www.ic3.gov/Media/News/2021/211101.pdf*

Setki tysięcy prób wykorzystania luki Log4Shell

14.12.2021 r. - 9 grudnia ujawniono poważną lukę w Log4j, bibliotece Apache powszechnie używanej przez twórców aplikacji internetowych i mobilnych. Firma Sophos wykryła już setki tysięcy prób ataków wykorzystujących tę podatność, m.in. z pomocą kryptominerów, czyli złośliwych programów służących do kopania kryptowalut. Według badaczy cyberprzestępcy będą w najbliższych tygodniach intensyfikowali działania i wykorzystywali lukę m.in. do ataków ransomware. Zagrożone mogą być setki tysięcy firm na całym świecie.

Nowe rodzaje ataków na horyzoncie

Luka nazwana Log4Shell umożliwia cyberprzestępcom zdalne wykonanie kodu, zainstalowanie złośliwego oprogramowania na urządzeniu ofiary, a nawet uzyskanie kontroli nad jej systemem. Na początku cyberprzestępcy wykorzystywali ją głównie w atakach przeprowadzanych za pomocą kryptominerów i botnetów. Badacze Sophos zaobserwowali także próby kradzieży danych z niektórych usług – m.in. kluczy do kont Amazon Web Services.

Trudności w znalezieniu luki

Powszechne wykorzystanie biblioteki Log4j w usługach i aplikacjach sprawia, że luka Log4Shell jest wyjątkowo trudna do wykrycia i załatania. Wiele podatności ogranicza się do konkretnych produktów lub platformy – np. luka ProxyLogon i ProxyShell w Microsoft Exchange. Jednak Log4Shell dotyczy oprogramowania, które jest wykorzystywane przez wiele rozwiązań i produktów. Może więc być obecna w wielu miejscach firmowych sieci i systemów, nawet w oprogramowaniu tworzonym na użytek wewnętrzny.

Polska trzecim „najbardziej dotkniętym" na świecie krajem pod względem prób wykorzystania luki Log4j do cyberataków

16.12.2021 r. - Zespół analityków ESET na bieżąco rejestruje przypadki mające na celu wykorzystanie luki Log4j. To odkryty w listopadzie poważny błąd w popularnej bibliotece języka programowania Java służącej do zbierania logów z aplikacji, która jest powszechnie używana m.in. w usłudze Apple iCloud, usługach Amazon, na platformie Twitter czy w grach, jak np. Minecraft. Odryty błąd naraża serwery na całym świecie na ryzyko ich całkowitego przejęcia przez cyberprzestepców.

Według aktualnych danych ekspertów ESET, Polska zajmuje trzecie miejsce na świecie pod względem częstotliwości prób wykorzystania do cyberataków luki Log4j.

Niebezpieczeństwo związane z luką Log4j jest powszechne, gdyż biblioteka Log4j jest szeroko stosowana, jako element wielu aplikacji opracowanych w języku Java. To narzędzie wykorzystywane przez największe światowe firmy technologiczne m.in. Apple, Microsoft, Cisco czy Amazon. Według ekspertów ESET częstotliwość wykrywania nadużyć związanych z luką jest zdumiewająca. Od momentu jej wykrycia potwierdzono kilkaset tysięcy prób takich incydentów. Najwięcej zarejestrowano dotychczas w Japonii i Stanach Zjednoczonych. Podium tego zestawienia zamyka Polska.

Sytuacja w naszym kraju jest bardzo podobna do innych państw rozwiniętych. Spowodowane jest to faktem, że próby ataków dotyczą organizacji i dostawców usług korzystających na co dzień z rozwiązań cyfrowych, wykorzystujących bibliotekę Apache Log4j.

Informacje na temat luki w bibliotece Apache Log4j (CVE-2021-44228) zostały udostępione publicznie 9 grudnia. To poważny incydent związany z cyberbezpieczeństwem, gdyż naraża niezliczone serwery na całym świecie na ryzyko ich całkowitego przejęcia przez cyberprzestepców. Wykorzystanie luki umożliwia hakerom zdalne wykonanie kodu (RCE) poprzez przesłanie i uruchomienie go na atakowanym serwerze, a w konsekwencji przejęcie nad nim kontroli. Skuteczne wykorzystanie luki grozi infekcją złośliwym oprogramowaniem serwera wybranej organizacji i może doprowadzić do jej paraliżu.

Jeśli atakujący dostanie się do sieci lokalnej, to może wykorzystać nawet systemy wewnętrzne, które nie są podłączone do Internetu. Haker nie potrzebuje fizycznego dostępu, aby uruchomić dowolny kod, który mógłby prowadzić do pełnej kontroli nad dotkniętymi nią systemami i kradzieży poufnych danych. Wykryta luka uzyskała 10 punktów w skali CVSS (system punktowania podatności w skali od 0-10 wykorzystywany do określenia poziomów ważności wykrytych luk).

Eksperci ESET zalecają administratorom systemów natychmiastowe sprawdzenie, czy uruchamiane przez nich aplikacje korzystają z podatnej na ataki biblioteki Log4j. Jeśli odnajdą taką aplikację w swoim systemie, biblioteka Log4j musi zostać natychmiast zaktualizowana do najwyższej wersji 2.16.0 (zagrożone podatnością są wszystkie wersje Log4j od 2.0 do 2.15.0 włącznie), zwłaszcza w przypadku jeśli aplikacja jest dostępna przez Internet. Następnie należy dokładnie sprawdzić, czy system nie został już naruszony. Pomogą w tym narzędzia udostępione w sieci.

Kaspersky rozszerza współpracę ze Scuderia Ferrari i zostaje partnerem zespołu e-sportowego tej marki

kaspersky

20.12.2021 r. - Kaspersky, czołowa globalna firma z branży cyberbezpieczeństwa, ogłosiła przedłużenie umowy partnerskiej ze Scuderia Ferrari. Ponadto firma Kaspersky dołączyła do partnerów e-sportowego zespołu FDA firmy Ferrari, który rywalizuje w światowej serii e-sportowej (Esports Series).

Jewgienij Kasperski, dyrektor generalny firmy Kaspersky, oraz Benedetto Vigna, dyrektor generalny firmy Ferrari

Partnerstwo pomiędzy firmą Kaspersky a Scuderia Ferrari rozpoczęło się w 2010 r., z roku na rok rozszerzając swój zakres. Kierując się wspólnymi wartościami, takimi jak doskonałość technologiczna, praca zespołowa oraz pasja do innowacji, firmy te zdołały zbudować silne i stabilne relacje, obejmujące również partnerstwo technologiczne. Kaspersky zapewnia firmie Ferrari światowej klasy cyberbezpieczeństwo oraz ochronę danych w trybie 24/7 na każdym etapie – od jej głównej fabryki w Maranello, we Włoszech, po wyścigi Formuły 1 na całym świecie.

Nowo podpisana wieloletnia umowa sponsorska stanowi kolejny kamień milowy w tej współpracy. Logo firmy Kaspersky nadal będzie widniało na kaskach kierowców oraz elementach wizualnej identyfikacji marki prezentowanych przez zespół, a także pojawi się na przednim skrzydle bolidów zespołu Scuderia Ferrari.

Poza przedłużeniem kontraktu ze Scuderia Ferrari firma Kaspersky stała się również oficjalnym partnerem zespołu e-sportowego FDA, założonego przez Ferrari w 2019 r., który rywalizuje w wyścigach Formula One Esports Series. Zespół ten skupia młode talenty i najszybszych

e-kierowców na świecie, do których należą Brendon Leigh, David Tonizza oraz Domenico Lovece.

Logo Kaspersky pojawi się na kombinezonach kierowców zespołu e-sportowego Ferrari oraz na flagowym centrum treningowym zespołu w Maranello. Umowa przewiduje również obecność marki podczas rozgrywek – logo firmy Kaspersky będzie umieszczone na samochodach wyścigowych biorących udział w F1 Esports Series.

Więcej informacji na temat współpracy firmy Kaspersky ze Scuderia Ferrari znajduje się na stronie https://www.kaspersky.com/scuderiaferrari.

Telemedycyna a incydenty naruszenia bezpieczeństwa danych pacjentów

21.12.2021 r. - Globalne badanie firmy Kaspersky pokazuje, że w 30% placówek medycznych doszło do incydentu naruszenia bezpieczeństwa informacji osobowych podczas zdalnych konsultacji medycznych prowadzonych przez personel. Ponadto niemal połowa z badanych placówek uważa, że ich lekarze nie do końca rozumieją, w jaki sposób chronione są dane pacjentów. Jednocześnie 67% uważa, że sektor ochrony zdrowia powinien gromadzić jeszcze więcej informacji osobowych, aby umożliwić dalszy rozwój branży.

Incydenty naruszenia bezpieczeństwa danych nie zawsze są skutkiem działań przestępców – często dopuszczają się ich osoby z wewnątrz. Organizacje medyczne gromadzą, przetwarzają i udostępniają ogromne ilości wrażliwych danych, dlatego powinny zwracać szczególną uwagę na ich bezpieczeństwo.

Z badania firmy Kaspersky wynika, że zaledwie 17% placówek medycznych ma pewność, że większość lekarzy przeprowadzających konsultacje zdalne orientuje się, w jaki sposób chronione są dane ich pacjentów. Jednocześnie 70% organizacji medycznych wdraża specjalistyczne szkolenia mające na celu zwiększenie świadomości bezpieczeństwa IT. Liczby te mogą sugerować, że większość wdrożonych praktyk dotyczących edukacji na temat cyberbezpieczeństwa nie przystaje do rzeczywistości i nie obejmuje tematów, które byłyby najbardziej przydatne w codziennej praktyce lekarzy.

Co istotne, 54% respondentów przyznało, że niektórzy lekarze prowadzą konsultacje zdalne za pośrednictwem aplikacji, które nie są przeznaczone do wykorzystywania w telemedycynie, jak np. FaceTime, Facebook Messenger, WhatsApp, Zoom itp.

Mimo problemów z bezpieczeństwem danych lekarze uważają, że gromadzie danych jest jednym z najważniejszych aspektów rozwoju technologii medycznej. Niemal siedmiu na dziesięciu (67%) respondentów zgadza się, że niezbędne jest gromadzenie większej ilości danych niż obecnie w celu szkolenia sztucznej inteligencji i oferowania trafnej diagnozy. To oznacza, że placówki medyczne powinny wzmocnić swoje środki cyberbezpieczeństwa, aby przygotować się na nową erę medycyny cyfrowej.

W celu zminimalizowania ryzyka wewnętrznych incydentów oraz zapewnienia nowych perspektyw dla branży organizacje medyczne powinny dostosować swoją politykę cyberbezpieczeństwa, by była adekwatna do współczesnych potrzeb. Obejmuje to jasne wskazówki dotyczące stosowania zewnętrznych usług i zasobów, przemyślane zasady dostępu do danych i zasobów cyfrowych oraz stosowanie silnych haseł. Naturalnie, wszystkie te środki muszą być stosowane w praktyce i uzupełnione o wszechstronne szkolenie podnoszące świadomość z zakresu cyberbezpieczeństwa[17].

Pełny raport wykorzystany w tej informacji prasowej jest dostępny na stronie https://r.kaspersky.pl/MyurW.

[17] *https://asap.kaspersky.com/pl/ :*

Powrót do biura: jak zadbać o cyberbezpieczeństwo podczas powrotu personelu do pracy stacjonarnej

Piotr Kupczyk,
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska

Wiele firm rozpoczęło już popandemiczną organizację pracy swojego personelu, a pozostałe z pewnością wkrótce się tym zajmą. Chociaż wiele przedsiębiorstw nie podjęło jeszcze ostatecznej decyzji odnośnie nowych realiów pracy, nawet częściowy powrót do biura będzie wymagał podjęcia pewnych działań przez dział IT oraz specjalistów ds. bezpieczeństwa IT.

Przejście na pracę zdalną było trudne, jednak powrót do biura może okazać się równie problematyczny. Organizacje będą musiały cofnąć niektóre zmiany, co może być równie skomplikowane jak ich wdrożenie. Trzeba będzie również ponownie zabezpieczyć usługi wewnętrzne oraz spełnić potrzeby pracowników dotyczące rozwiązań, do których przyzwyczaili się podczas lockdownu. Rozważenia wymaga wiele kwestii, dlatego w tym artykule wymienię kilka działań dotyczących cyberbezpieczeństwa, które mogą pomóc firmom w odpowiednim rozłożeniu sił.

1. Utrzymaj zabezpieczenia wprowadzone dla pracy zdalnej

Aby zapewnić bezpieczeństwo korporacyjnych punktów końcowych podczas pracy zdalnej, firmy najprawdopodobniej wprowadziły dodatkowe środki ochrony, takie jak kontrola bezpieczeństwa oraz scentralizowane zarządzanie poprawkami na komputerach zdalnych, konfiguracja lub rozszerzenie połączenia VPN oraz specjalistyczne szkolenia w celu zwiększenia świadomości bezpieczeństwa. Istotną rolę odgrywały technologie wykrywania i reagowania na punktach końcowych, wypełniając luki w ochronie, która mogła nie działać tak dobrze w związku z faktem, że część urządzeń funkcjonowało poza granicami sieci korporacyjnej.

Praktyki te powinny nadal obowiązywać dla hybrydowych modeli pracy – gdy pracownicy przechodzą z biur domowych do pracy na miejscu lub podróżują służbowo. Dzięki stosowaniu połączeń VPN, rozwiązań EDR oraz systemów wykrywania włamań na punktach końcowych pracownicy będą mogli bezpiecznie pracować niezależnie od miejsca, w którym wykonują swoje zadania.

2. Uważnie rozplanuj zasoby oraz czas na aktywowanie zabezpieczeń, które zostały wyłączone dla pracy zdalnej

Aby umożliwić pracownikom zdalne łączenie się z siecią firmową, szczególnie z urządzeń prywatnych, organizacje mogą osłabić lub wyłączyć niektóre mechanizmy kontroli zabezpieczeń – takie jak Network Admission Control (NAC). NAC sprawdza, czy komputery spełniają korporacyjne wymogi bezpieczeństwa, zanim zezwoli im na dostęp do sieci firmowej. Jeśli dany komputer nie jest autoryzowany, posiada nieuaktualnione oprogramowanie antywirusowe lub w inny sposób nie spełnia wymogów, NAC nie zezwoli mu na dostęp do sieci, dopóki problemy te nie zostaną rozwiązane.

Gdy pracownicy wrócą do biura i połączą się z siecią korporacyjną, NAC powinien zostać włączony, aby chronić wewnętrzne systemy na wypadek, gdyby maszyny stanowiły jakiekolwiek zagrożenie. Ponieważ przez długi czas komputery były wykorzystywane do pracy zdalnej, pewne aktualizacje mogły zostać pominięte. To oznacza, że włączenie NAC dla dziesiątek, a nawet setek takich maszyn może spowodować liczne błędy. Dlatego włączenie tej usługi może być procesem realizowanym krok po kroku i dostosowywanym do niewielkiej grupy pracowników.

Organizacje powinny przewidzieć takie problemy i posiadać plan, który uwzględnia zasoby, terminy, usuwanie błędów, a nawet pomoc integratorów IT.

3. Zapewnij aktualizacje wewnętrznych systemów

Nie zapomnij sprawdzić wewnętrznych usług o znaczeniu krytycznym. Jeśli istnieją niezałatane serwery, lepiej, aby zespół ds. bezpieczeństwa IT wiedział o nich, zanim pracownicy wrócą do biura.

Przed pandemią, gdy wszyscy jeszcze pracowali w biurze, komputery były stale połączone z siecią firmową oraz objęte ochroną w trybie 24/7. Dlatego ryzyko przeniknięcia do sieci exploita z komputera PC oraz wykorzystania przez niego luk w podatnym na ataki serwerze było niższe.

A teraz wyobraź sobie, że wszyscy pracownicy wrócili do biura w jednym czasie, podłączając swoje laptopy do sieci firmowej, a jednocześnie istnieje niezałatany kontroler domen, który zarządza kontami wszystkich użytkowników. Jeśli wśród setek urządzeń będą takie, które zostały zainfekowane, i cyberprzestępcy odkryją podatny na ataki kontroler, będą mogli uzyskać dostęp do danych dotyczących kont pracowników, jak również ich haseł. Miejmy nadzieję, że zespół ds. bezpieczeństwa IT zdoła szybko wykryć problem, ale i tak czeka go dodatkowa praca związana z reorganizacją sieci i zmianą wszystkich haseł.

4. Przygotuj się na oszczędności, jak również koszty

Powrót pracowników do biur pozwoli pracodawcom zaoszczędzić nieco pieniędzy. Na przykład, w firmie Kaspersky zwiększono liczbę tuneli VPN z 1 000 do 5 000 – 8 000, aby większość pracowników mogła pracować z domu. Gdy wrócą do biura, tak duża liczba licencji na połączenia VPN nie będzie potrzebna, co pozwoli obniżyć wydatki z tego tytułu.

Podobnie, firmy mogą zmniejszyć liczbę opartych na subskrypcji rozwiązań w chmurze, takich jak np. Slack czy Microsoft Teams. Nie będzie potrzeby posiadania tak wielu licencji w chmurze – z niektórych usług znów będzie można korzystać lokalnie. To samo może dotyczyć aplikacji związanych z podpisami cyfrowymi. O ile w czasie lockdownu były one konieczne, teraz, po zniesieniu ograniczeń dotyczących przemieszczania się, można zmniejszyć ich liczbę i połączyć z tradycyjnym procesem podpisywania dokumentów.

5. Zachowaj narzędzia i ustawienia, z którymi pracował personel

Wykonując swoje obowiązki zdalnie, pracownicy opanowali nowe narzędzia komunikacji i współpracy – czaty, wideokonferencje, narzędzia do planowania, oprogramowanie do zarządzania relacjami z klientami. Z pewnością będą chcieli nadal z nich korzystać, bo są już im dobrze znane i wygodne. Jak wynika z jednego z badań[1] firmy Kaspersky, pandemia sprawiła, że 74% osób chce elastyczniejszych i wygodniejszych warunków pracy.

Zakazanie pracownikom korzystania z takich innowacji może nie być mądrą decyzją. Mogłoby nasilić zjawisko określane jako „shadow IT", gdy pracownicy korzystają z aplikacji na własną rękę bez zezwolenia działu IT. Firmy powinny zezwolić na korzystanie z nowych usług lub zaproponować alternatywy oraz wyjaśnić personelowi, dlaczego należy wybierać bezpieczniejsze możliwości. Istnieją specjalne rozwiązania, które pomagają organizacjom zarządzać dostępem do usług w chmurze – specjalne funkcje Cloud Discovery w rozwiązaniu zabezpieczającym czy brokery zabezpieczeń dostępu do chmury – które egzekwują polityki bezpieczeństwa dla chmur.

Bezpieczeństwo IT powinno wspomagać firmę, a nie ograniczać ją. Zignorowanie zmiany modelu pracy może wpłynąć na to, jak pracownicy będą postrzegać firmę. Pozwalając im na większą elastyczność pracy oraz korzystanie z wygodnych dla nich usług, firma może zyskać na atrakcyjności nie tylko w oczach obecnych pracowników, ale również przyszłych potencjalnych kandydatów. I na odwrót: odrzucenie takich zmian może prowadzić do braku aprobaty ze strony personelu oraz opinii publicznej w przypadku ujawnienia stanowiska firmy w tym zakresie.

Pandemia oraz przejście na pracę zdalną stanowiły wyzwania wynikające z siły wyższej. Coś takiego nie zdarza się często. Mimo trudności wszyscy zdobyliśmy bezcenne doświadczenie i odebraliśmy ważne lekcje na przyszłość.

Jedna z najważniejszych lekcji dotyczy tempa transformacji biznesu oraz elastyczności technologii informatycznych. Osoby odpowiedzialne za bezpieczeństwo IT nie powinny stosować zakazów, a bardziej proponować opcje oraz wspomagać elastyczność. Przemyślany i bezpieczny powrót do pracy w biurze w dowolnej formie może pomóc firmom wykorzystać ten trend.

[1] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3333*

Stacje paliw i nie tylko: dlaczego cyberbezpieczeństwo stanowi najwyższy priorytet dla infrastruktury przemysłowej

Piotr Kupczyk, Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska

Przemysłowe systemy sterowania (ang. Industrial Control Systems, ICS), ze względu na swą złożoną strukturę, podłączone urządzenia, oprogramowanie i systemy operacyjne, jak również krytyczne funkcje, wymagają specjalnego podejścia w zakresie cyberbezpieczeństwa. Nie tylko w teorii.

Jako przykładu użyjmy czegoś tak powszechnego jak stacja paliw. Stacja taka ma wszelkie atrybuty systemu ICS: połączony sprzęt, w tym pompy i zbiorniki, kontrolery, system zarządzania, system płatności, jak również połączenie z siecią firmową, zewnętrznymi systemami usług oraz internetem. Jak każdy obiekt przemysłowy, stacja paliw jest obarczona pewnymi problemami dotyczącymi cyberbezpieczeństwa, o których należy wiedzieć, aby nie spowodowały zakłóceń mogących wpłynąć na funkcjonowanie obiektu, na jego pracowników czy też na inne osoby. Przykładem takiego zagrożenia może być niedawny incydent[1], w którym na skutek ataku ukierunkowanego zamknięto stacje paliw w Iranie.

Prezentowany w niniejszym artykule przegląd infrastruktury ICS opiera się na badaniu[2], które eksperci z firmy Kaspersky przeprowadzili pod koniec 2020 r. Obejmowało ono analizę współczesnej architektury oprogramowania do automatyzacji stacji paliw, typowej infrastruktury oraz komunikacji wewnątrz niej. Badanie to umożliwiło nam klasyfikację potencjalnych wektorów ataków oraz ich wpływu na sieć stacji paliw.

Wizyta na stacji paliw

Wyobraź sobie, że jedziesz samochodem i musisz go zatankować. Zatrzymujesz się na stacji, umieszczasz dystrybutor w baku i idziesz do kasy, by zapłacić za paliwo. W sklepie na stacji przyjemnie pachnie świeża kawa, wybierasz więc kilka przekąsek na drogę, finalizujesz zakup i wracasz do samochodu.

Aby w Twoim baku mogło znaleźć się paliwo, niezbędne jest działanie kilku systemów. System back-office oraz punkty sprzedaży są wykorzystywane do obsługi płatności oraz zarządzania. Są one połączone z kontrolerem placu parkingowego, czyli terenu z pompami przed sklepem stacji paliw, na którym klienci parkują swoje samochody w celu zatankowania. Jest on wyposażony w wiele systemów, takich jak kontrola pomp, automatyczny wskaźnik poziomu paliwa, systemy płatności itd. Kontroler placu parkingowego to główne urządzenie zarządzające dystrybucją paliwa – gdy bak jest pełny, system automatycznie przekazuje informację do pompy, by przestała tłoczyć paliwo, a kasjer otrzymuje stosowną informację w swoim systemie. Podobnie dzieje się, gdy samodzielnie zatrzymasz tankowanie.

Informacje dotyczące operacji, jak również ilości sprzedanego i dostępnego paliwa są przekazywane do systemu zarządzania lokalnie, a następnie do centrali, która gromadzi informacje ze wszystkich stacji.

Gdzie pojawiają się problemy?

Dzięki badaniu naszym ekspertom udało się ustalić, co może pójść nie tak w tym procesie. Istnieje kilka potencjalnych problemów dotyczących technologii operacyjnej (OT) oraz cyberbezpieczeństwa, które mogą wpłynąć na pracę stacji paliw.

Pierwsza grupa zagrożeń dotyczy uzyskania zdalnego dostępu z zewnętrznych sieci. Jak wiele współczesnych systemów przemysłowych, stacja paliw stosuje rozwiązania, które są połączone z publicznymi usługami za pośrednictwem internetu, np. systemy bankowości w chmurze czy wyspecjalizowane systemy zarządzania flotą. Zdalny dostęp do stacji paliw umożliwia dalsze szkodliwe działania wewnątrz sieci.

Zdarzyło się tak w przypadku opisanym w jednym z badań[3] firmy Kaspersky. Na stacji paliw wykorzystywano oprogramowanie do zarządzania paliwem, które umożliwiało monitorowanie ilości paliwa na stanie, ustalania ceny i przetwarzanie płatności. System ten był połączony z internetem i miał luki w zabezpieczeniach, za pośrednictwem których możliwe było uzyskanie zdalnego dostępu na poziomie administratora, pozwalającego nawet zmienić cenę paliwa.

Dostęp do niektórych części infrastruktury posiadają określeni dostawcy i firmy usługowe. Złamanie zabezpieczeń systemów takich osób trzecich może otworzyć cyberprzestępcom drzwi do atakowanego systemu. Ten rodzaj zagrożenia stanowi ogromny problem dla firm dowolnej wielkości: jedna trzecia (32%) dużych organizacji doświadczyła ataków mających związek z danymi współdzielonymi z dostawcami[4]. Co więcej, straty finansowe poniesione przez przedsiębiorstwa w wyniku takich incydentów w 2021 r. były najwyższe spośród wszystkich rodzajów ataków.

Kolejna grupa zagrożeń dotyczy problemów sieciowych oraz urządzeń, które mogą potencjalnie prowadzić do zakłócenia działania stacji paliw lub do bezpośrednich strat finansowych. Ataki mogą pochodzić ze zdalnych sieci lub być następstwem połączenia się z sieciami bezprzewodowymi lub lokalnymi przewodowymi portami sieciowymi.

Następnie, jeśli sieć nie jest segmentowana, atak może rozprzestrzenić się z punktów wejścia, takich jak pomocniczy

sprzęt w sklepie czy biurowe stacje robocze, do komponentów krytycznych, takich jak kontrolery zarządzania paliwem. Stosowanie niezaszyfrowanych protokołów (HTTP, CDP, FTP, Telnet itd.) w sieci stacji paliw może umożliwić atakującym przechwycenie wrażliwych informacji, które zostaną wykorzystane w dalszych etapach ataku.

Innym krytycznym, a zarazem wciąż aktualnym problemem są luki lub błędy w zabezpieczeniach kontrolera paliwa, terminali płatniczych oraz sprzętu sieciowego, jak również korporacyjnych punktów końcowych oraz aplikacji. W 2015 r. wykryto[5], że 5 800 automatycznych wskaźników poziomu paliwa było narażonych na nieautoryzowany dostęp z internetu z powodu braku ochrony za pomocą hasła na porcie szeregowym. Wskaźnik tego typu to elektroniczny komponent umieszczany w zbiorniku, który monitoruje poziom paliwa i sprawdza, czy nie wystąpił przeciek. Za pomocą portu szeregowego możliwe jest zaprogramowanie wskaźnika. Jeśli przesyłany sygnał nie jest prawidłowy, operator nie otrzyma alertu o odstępstwie od normy. Dane z 2015 r. sugerowały ponadto, że większość takich systemów w tym czasie znajdowała się na stacjach paliw w Stanach Zjednoczonych i stanowiła 3% urządzeń wykorzystywanych w tym kraju. Złamanie zabezpieczeń tak krytycznych systemów jak automatyczne wskaźniki poziomu paliwa może umożliwić przestępcom przeprowadzenie oszustw, a nawet wyrządzenie fizycznych szkód.

Niezmiernie ważne jest także kontrolowanie wszystkich stacji roboczych wykorzystywanych na stacji paliw, takich jak punkty sprzedaży, systemy back-office, kontrolery paliwa czy terminale płatności, jak również ich konfiguracji, a nawet dostępu do portów USB. Na przykład, brak szyfrowania lub spełnienia określonych standardów w systemie płatności może narazić go na atak. W przypadku kontrolera paliwa należy sprawdzić protokoły przemysłowe. Brak uwierzytelnienia źródła lub kontroli integralności może umożliwić cyberprzestępcom przeprowadzającym przechwycenie danych oraz manipulację kontrolerami stacji.

Kolejnym elementem wymagającym zarządzania są bezprzewodowe bramy oraz urządzenia do odczytu. Należy przeprowadzić ocenę bezpieczeństwa w celu zidentyfikowania niezabezpieczonych protokołów przemysłowych czy możliwości przeprowadzenia ataków zagłuszających komunikację.

Jak zwiększyć poziom bezpieczeństwa

Istnieją podstawowe środki bezpieczeństwa mogące pomóc podnieść ogólny poziom infrastruktury technologii operacyjnej. Oprócz tego, że mają one zastosowanie do stacji paliw, są równie istotne w odniesieniu do dowolnej sieci przemysłowej.

Bezpieczeństwo sieci: celowa segmentacja sieci zwiększa ogólne bezpieczeństwo i minimalizuje powierzchnię potencjalnych ataków. Segment sieci, który ma dostęp do jej niezaufanych części, takich jak korporacyjna infrastruktura IT, również powinien zostać odseparowany i chroniony przy pomocy odpowiedniego oprogramowania zabezpieczającego klasy biznesowej.

Pasywne monitorowanie sieci OT jest niezbędne dla inwentaryzacji zasobów oraz komunikacji, jak również wykrywania włamań, zanim wpłyną one na proces technologiczny. Dane monitorowania pozwalają również zespołom bezpieczeństwa IT analizować zdarzenia i rozważyć ograniczenie funkcjonalności, co może dodatkowo zwiększyć bezpieczeństwo.

Kontrola dostępu: powinna obejmować ograniczenie fizycznego i logicznego dostępu do systemu automatyzacji oraz kontroli. Środki bezpieczeństwa mające na celu kontrolę zdalnego dostępu uzyskiwanego przez firmy usługowe pomogą zapobiec incydentom za pośrednictwem podmiotów trzecich.

Ochrona punktów końcowych: należy wdrożyć wyspecjalizowane oprogramowanie bezpieczeństwa klasy przemysłowej dla urządzeń i serwerów OT. Ponadto należy upewnić się, że oprogramowanie jest zatwierdzone przez producenta systemu automatyzacji i kompatybilne z jego rozwiązaniami. Pozwoli to uniknąć sytuacji, w której produkt zabezpieczający oddziałuje na funkcje operacyjne.

Zarządzanie bezpieczeństwem: należy wdrożyć system do scentralizowanego gromadzenia zdarzeń dot. bezpieczeństwa oraz zarządzanie zasadami związanymi z oprogramowaniem bezpieczeństwa. Istotne jest również, aby rozwiązanie umożliwiało zarządzanie lukami w zabezpieczeniach oraz poprawkami. Możliwość zintegrowania systemu z zarządzaniem informacjami i zdarzeniami bezpieczeństwa (SIEM) jest przydatną opcją dla organizacji, które planują zwiększyć swój poziom ochrony. Ciągłe monitorowanie w czasie rzeczywistym oraz gromadzenie danych z punktów końcowych wraz z możliwościami reagowania i analizy w oparciu o reguły pomoże osiągnąć jeszcze lepszą ochronę przed zaawansowanymi atakami.

Poprawa ogólnego poziomu cyberbezpieczeństwa wymaga również bardziej fundamentalnego podejścia obejmującego działania długoterminowe. Oznacza to przestrzeganie standardów przemysłowych dla kontroli bezpieczeństwa informacji, takich jak IEC 62443, NIST, NERC CIP itd. Organizacja powinna również regularnie przeprowadzać testy penetracyjne lub analizę bezpieczeństwa w celu zidentyfikowania luk w zabezpieczeniach oraz problemów dot. bezpieczeństwa informacji, zanim zostaną przez kogoś wykorzystane. I oczywiście przestrzegać wszystkich zalecanych środków w celu usunięcia takich luk.

W zależności od poziomu ochrony danej firmy można mówić o bardziej szczegółowych wymaganiach. Niemniej jednak wymienione wyżej działania mają zasadnicze znaczenie dla usunięcia większości luk w cyberbezpieczeństwie. Czy chodzi o stację paliw, rafinerię czy dużego producenta samochodów, podstawowe zasady ochrony OT oraz IT powinny umożliwić firmie przygotowanie niezawodnego systemu cyberbezpieczeństwa oraz rozwijanie go zgodnie z indywidualnymi potrzebami. To świetny fundament, na którym można budować satysfakcję zarówno właścicieli przedsiębiorstw, jak i ich klientów.

[1] *https://www.forbes.com/sites/thomasbrewster/2021/10/26/iran-gas-stations-stop-pumping-petrol-after-cyberattack-reports-state-media/*
[2] *https://ics-cert.kaspersky.com/publications/reports/2018/02/07/gas-is-too-expensive-lets-make-it-cheap/*
[3] *https://www.kaspersky.pl/o-nas/informacje-prasowe/2927*
[4] *https://calculator.kaspersky.com/app/report*
[5] *https://threatpost.com/thousands-of-us-gas-stations-vulnerable-to-remote-hacks/110608/*

Kwestie bezpieczeństwa głównym powodem, dla którego firmy nie wdrażają chmury obliczeniowej

Artur Józefiak, dyrektor Accenture Security w Polsce i Europie Środkowo-Wschodniej

Olga Budziszewska, manager ds. bezpieczeństwa chmury w Accenture

- **65% przedstawicieli wyższej kadry zarządzającej z działów IT jako największą przeszkodę w czerpaniu pełnych korzyści z chmury wskazało ryzyka związane z zapewnieniem bezpieczeństwa przetwarzanych informacji oraz zgodności sposobu i zakresu tego przetwarzania z prawem. Te same zagadnienia są również największą barierą dla wdrożenia chmury w organizacjach.**
- **Firmy w Polsce coraz odważniej podchodzą do wykorzystania chmury obliczeniowej w codziennej działalności, ale wciąż inwestują w nią fragmentarycznie. Zmagają się też z niedoborem kadr.**
- **Lukę w zatrudnieniu w obszarze cyberbezpieczeństwa szacuje się globalnie na 4,07 mln osób, a w samej Europie na blisko 300 tys. pracowników[1].**

Wiele firm upatruje szansy na rozwój w wykorzystaniu chmury obliczeniowej w bieżącej działalności. Wśród głównych atutów wskazywane są takie kwestie jak wydajność, skalowalność oraz wspieranie innowacyjności. Ostatni rok jednoznacznie pokazał, jak istotna jest dla organizacji odporność systemów, ich zwinność oraz potencjał do adaptacji. Wiele firm wstrzymuje się jednak z opracowaniem strategii oraz faktyczną migracją do chmury przede wszystkim ze względów bezpieczeństwa. Sytuacji nie ułatwiają wymagania regulacyjne, niedobór kadr oraz brak holistycznego podejścia do inwestycji w chmurę.

Według raportu[2] firmy ISC lukę w zatrudnieniu w obszarze cyberbezpieczeństwa szacuje się globalnie na 4,07 mln osób, a w samej Europie brakuje blisko 300 tys. pracowników i tendencja jest wzrostowa. Potwierdza to także raport „Bezpieczna chmura: Jak zadbać o bezpieczeństwo organizacji w czasie migracji do chmury obliczeniowej?" przygotowany przez firmę Accenture, który dodatkowo naświetla kwestię niedoboru specjalistów ds. chmury obliczeniowej i cyberbezpieczeństwa.

W Polsce dominują dwa skrajne podejścia do korzystania z rozwiązań chmurowych. Część organizacji, głównie z sektorów o mniejszych wymaganiach regulacyjnych, rozpoczyna szerokie zastosowanie chmury, często pomijając całościową analizę ryzyka i wprowadzenie obowiązkowych zmian w obszarze bezpieczeństwa wynikających z różnic w korzystaniu z chmury względem architektury on-premise. Natomiast pozostałe przedsiębiorstwa, w obawie przed utratą bezpieczeństwa danych lub niezgodnością regulacyjną, opóźniają adopcję rozwiązań chmurowych, jednocześnie rezygnując z korzyści z nimi związanych. Szczególnie istotną zaletą chmury jest szybsza i tańsza adopcja innowacji technologicznych, co w gospodarce cyfrowej jest kluczowym źródłem przewagi konkurencyjnej. W ten sposób słuszne, ale niezaadresowane prawidłowo obawy o bezpieczeństwo chmury stają się powodem obniżenia konkurencyjności polskich firm. Rozwiązaniem jest opracowanie całościowej koncepcji bezpieczeństwa rozwiązań chmurowych i – w kolejnym kroku – zbudowanie procesów oraz architektury bezpieczeństwa dostosowanych do rzeczywistości usług chmurowych. Na przeszkodzie jednak stają konieczność podjęcia się inwestycji na początku procesu oraz brak doświadczenia i niedobór wyspecjalizowanej kadry świadomej wyzwań dot. bezpieczeństwa chmury.

Problem niedoboru kadr można rozwiązać częściowo za pomocą automatyzacji i procesów samoregeneracji, które zmniejszają liczbę czynności wykonywanych ręcznie. Powinny jednak temu towarzyszyć inwestycje w szkolenie już zatrudnionych pracowników. Kluczowe jest odpowiednie nastawienie osób odpowiedzialnych za bezpieczeństwo informatyczne i mentoring w organizacji. Spośród zbadanych przez Accenture firm, 30% liderów technologicznych przeszkoliło trzy czwarte pracowników, kiedy pojawiło się zapotrzebowanie na nowe umiejętności. Jednocześnie wśród organizacji mniej zaawansowanych technologicznie zrobiło to tylko 9%. Inwestycje we własnych programistów, którzy już posiadają niezbędne zaplecze kompetencji, by szybko rozszerzyć swoje umiejętności w zakresie bezpieczeństwa w chmurze, są równie ważne jak nakłady na nowe technologie.

Kolejnym wyzwaniem dla firm w drodze do bezpiecznego wdrożenia rozwiązań chmurowych jest brak kompleksowego podejścia w strategiach przejściowych, co najczęściej jest związane z niewystarczającymi inwestycjami. Tylko 40% firm twierdzi, że osiąga pełną wartość oczekiwaną z inwestycji w chmurę. Według 65% przedstawicieli wyższej kadry zarządzającej z działów IT przeszkodę w czerpaniu pełnych korzyści z chmury stanowi ryzyko związane z bezpieczeństwem i zapewnieniem zgodności z wymogami regulacyjnymi. Zabezpieczenie chmury różni się zasadniczo od ochrony środowisk lokalnych. O bezpieczeństwo hybrydowych, wielochmurowych środowisk obliczeniowych musi zadbać zarówno sama organizacja, jak i dostawcy usług chmurowych. Ich funkcją jest zabezpieczenie infrastruktury i aktualizacja natywnych funkcji bezpieczeństwa dla firm korzystających z rozwiązania Platform-as-a-Service. Z kolei zadaniem organizacji jest opracowanie strategii i sposobów monitorowania wykorzystywanych przez nią środowisk chmurowych od różnych dostawców, tak aby spełniały one wymagania regulatora i możliwe było wyłapanie wszystkich nieprawidłowości.

Podobnie jak infrastruktura on-premise, chmura wymaga dedykowanych narzędzi i kompetencji w obszarze cyberbezpieczeństwa. Powinna być traktowana jak pozostałe elementy cyklu życia i rozwoju oprogramowania, a zmiany muszą być wprowadzane w taki sam sposób, jak w każdej aplikacji – poprzez sprawdzanie i usuwanie kodu. Jeśli nie uda się nam wprowadzić efektywnej zmiany w podejściu do bezpieczeństwa, niedostateczna harmonizacja działań, słabe zarządzanie, ręczne procesy, narzędzia starszej generacji oraz braki w kompetencjach sprawią, że kadra kierownicza zacznie postrzegać kwestie bezpieczeństwa jako hamulec dla rozwoju firmy.

Bez formalnej strategii i centralnego zarządzania zmianami firmy mogą zmagać się z nadmiarem pracy i powielaniem rozwiązań kontrolnych, słabą komunikacją, wyższymi kosztami i wydłużeniem czasu osiągnięcia wartości. Brak strategii skutkuje również reaktywnym podejściem do bezpieczeństwa. Nie wystarczy samo wysyłanie alertów o incydentach sygnalizujących luki w zabezpieczeniach. Architektura referencyjna bezpieczeństwa powinna zawierać narzędzia kontroli prewencyjnej w celu zablokowania przypadkowych lub złośliwych incydentów bezpieczeństwa jeszcze przed ich wystąpieniem. Warto od samego początku zadbać o bezpieczeństwo, aby uniknąć dodatkowych kosztów związanych z koniecznością naprawiania błędów. Bezpieczeństwo w chmurze powinno być integralną częścią strategii bezpieczeństwa całej organizacji.

Pełny raport „Bezpieczna chmura: Jak zadbać o bezpieczeństwo organizacji w czasie migracji do chmury obliczeniowej?" jest dostępny na stronie: https://www.accenture.com/pl-pl/insights/security/secure-cloud-poland.

[1] *ISC: Women in Cybersecurity. 2019 r.*
[2] *ISC: Women in Cybersecurity. 2019 r.*

BGP, DNS i kruchość naszych systemów krytycznych Awaria Facebooka – spekulacje: DNS i BGP w grze

Ireneusz Wiśniewski,
dyrektor zarządzający
F5 Poland

Serwisy Facebooka doświadczyły poważnej, sześciogodzinnej awarii. Usterka rozlała się na usługi powiązane z Facebookiem, w tym na komunikatory WhatsApp i Instagram oraz okulary Oculus VR. Biorąc pod uwagę skalę wydarzenia, przybliżamy zagadnienia wiążące się z problematyką niektórych technologii internetowych, na których tak mocno polegamy w życiu prywatnym i biznesie.

Zawsze chodzi o DNS…

System nazw domen (DNS) to pojedynczy punkt awarii systemów internetowych. DNS mapuje nazwy, takie jak facebook.com, na adresy IP, umożliwiając użytkownikom łatwe odwoływanie się do witryn (według nazwy).

W efekcie DNS zapewnia powiązanie nazw z adresami IP – jak książka adresowa. Gdy serwery DNS witryny nie działają, podobne wyszukiwanie nie może się odbyć, a użytkownicy nie będą mogli uzyskać dostępu do witryny. Utrzymanie sprawności, działania i bezpieczeństwa serwerów DNS jest więc kluczowym elementem niezawodności działania strony internetowej.

…chyba że chodzi o BGP

Pod pojęciem BGP kryje się inna technologia, która jest tak samo ważna jak DNS. Jest to protokół routingu (jeden z wielu) o nazwie Border Gateway Protocol (BGP). Umożliwia on Systemom Autonomicznym (zbiór dużych sieci kontrolowanych przez jeden podmiot) przekazywanie informacji o kontrolowanych przez siebie sieciach, dzięki czemu posiadają one spójną wiedzę o tym, jak dotrzeć do poszczególnych podsieci IP. BGP nie realizuje funkcjonalności routingu bezpośrednio, ale jest protokołem, który udostępnia informacje między routerami. Po otrzymaniu tych informacji routery mogą podejmować decyzje o tym, dokąd należy przesłać konkretne dane.

Dlaczego protokół BGP jest ważny?

Wpisując w przeglądarce internetowej dowolny adres strony, np. facebook.com, powodujemy, że komputer wykona wyszukiwanie DNS, a lokalny serwer DNS, z którego korzysta nasz komputer, powinien zwrócić odpowiedni adres IP.

Wtedy nasz komputer musi być w stanie kierować ruch na ten adres IP. Należy zauważyć, że decyzje dotyczące routingu są podejmowane na zasadzie krok-po-kroku. Każdy router po drodze, przez który przechodzą dane, zdecyduje, jaki powinien być następny krok trasy do docelowego adresu IP. W tym celu sprawdza tablicę routingu, żeby określić następne

miejsce do przesłania danych.

Jeśli router uczestniczy w protokole BGP, jego tablica routingu jest konstruowana na podstawie aktualizacji otrzymanych od innych routerów obsługujących BGP.

Obejmuje to informacje o tym, do jakich sieci można się dostać za pomocą poszczególnych routerów, a także jak blisko jest celu. W tym przypadku bliskość nie oznacza liczby routerów, ale liczbę Systemów Autonomicznych, przez które będą musiały być przesłane dane. Istnieje złożony algorytm używany do określenia, która z możliwych tras jest najlepsza. „Najlepsza" może również określać inne elementy, jak zasady dotyczące ruchu wychodzącego czy umowy tranzytowe między dostawcami usług internetowych. Jeśli okaże się, że tabela routingu pokazuje dwa routery, które mogą przesłać dane, aby dotrzeć do określonego adresu IP, wybierze jeden z dwóch na podstawie wskazanych wyżej czynników.

Podobne decyzje dotyczące routingu są podejmowane przez każdy router, który przesyła dane, przekazując je do innego routera lub określając bezpośrednie połączenie z siecią danego adresu IP, dostarczając dane do miejsca docelowego. Ten sam proces zostanie wykonany w odwrotnej kolejności, aby skierować ruch z powrotem przez inną serię routerów, a następnie do klienta.

Taki schemat ma wiele zalet. Dopóki dla ruchu dostępny jest router docelowy – a większość firm korzystających z internetu ma wiele takich routerów – nasze dane powinny (ostatecznie) tam trafić. Ruch pomiędzy daną witryną internetową a klientem jest dzielony na wiele pakietów, zatem mogą być one przesyłane różnymi trasami.

Jest to cecha pozwalająca na unikanie problemów z dostępnością witryn, gdyby jakiś pośredni router uległ awarii. Wtedy pakiety składające się na nasze żądanie lub odpowiedź mogą zostać przekierowane do działających routerów. Działa to dobrze, jeśli tablice routingu są spójne i zawierają poprawne informacje. W końcu internet został pierwotnie zaprojektowany do omijania ataków nuklearnych.

Obrazowe przedstawienie problemu

Wyobraźmy sobie, że chcemy dostać się do domu przyjaciela, ale nigdy tam nie byliśmy. Sprawdzamy adres – to jak część DNS. Teraz trzeba wymyślić, jak się tam dostać, więc udajemy się do najbliższego skrzyżowania i pytamy uczestników ruchu, w którą stronę powinniśmy się kierować. Uczestnicy ruchu podpowiadają, żeby skręcić w lewo. Podążamy tą drogą, aż przemieścimy się do kolejnego skrzyżowania, i pytamy o drogę ponownie. Dostajemy informację, aby kierować się w prawo.

Kontynuujemy proces, aż dotrzemy do celu. Możliwe, że dostaniemy po drodze instrukcję: „standardowo rekomendujemy trasę przez most, ale jest wyłączony z ruchu, więc należy kierować się w lewo i ponownie zapytać o drogę na następnym skrzyżowaniu". Możemy także dostać instrukcję: „trasa po skręcie w lewo jest bezpośrednia, ale skierowanie się w prawo i przejazd przez autostradę będzie szybszy".

Wybrana trasa nie zawsze będzie najprostszą, ani nawet najszybszą drogą do celu, ale pozwoli uniknąć blokad dróg, zawalonych mostów i korków na trasie. Jeśli zapytania o drogę będą kierowane do uczestników ruchu, którzy mają dobre informacje, dotrzemy do celu. Środkiem, za pomocą którego przekazywane są te dobre informacje, jest właśnie BGP. Jeśli BGP podaje nieprawidłowe informacje lub w ogóle nie ma informacji o tym, jak dotrzeć do obranego celu, mogą się zdarzyć utrudnienia.

Czy BGP jest bezawaryjny?

BGP jest solidny i dobrze się skaluje, co jest kluczową funkcją przy próbach połączenia miliardów hostów. Nie jest jednak całkowicie bezawaryjny.

Wyznaczona trasa może pomijać drogi, które powinny się na trasie znaleźć. Oznacza to, że powiązana sieć po prostu przestaje być w internecie widoczna (znika z niego). Siłą rzeczy nie wiadomo, jak się tam dostać, a ruch przeznaczony do tej sieci zostanie odrzucony.

Czasami robi się to celowo – nazywa się to blackholing – i zwykle ma na celu zablokowanie połączeń do lub z danej sieci. Dzieje się tak w wielu przypadkach. Na przykład celem zablokowania ruchu DDoS z wrogiej sieci lub nawet usunięcia całego kraju z internetu w czasie kryzysu cywilnego. W rezultacie ruch sieciowy jest po prostu usuwany, często bez powiadomienia zwrotnego do nadawcy. Sieć zablokowana przez blackholing nie będzie otrzymywać ruchu i zostanie skutecznie odcięta od (cyfrowego) świata.

Trasa może być również nieprawidłowo wskazana. Błędna konfiguracja ze strony Systemu Autonomicznego może sprawiać wrażenie, że kieruje ruch do sieci, których nie kontroluje. Gdy jest to działanie celowe, nazywa się je BGP hijacking i chociaż istnieją przed tym zabezpieczenia, powoduje to przekierowanie dużej ilości ruchu do bardzo różnych miejsc, np. celem przechwytywania i badania ruchu w ramach działań szpiegowskich.

Takie przypadki są częste. Na przykład operator sieci lub zautomatyzowany system dokonują błędnej konfiguracji. Niezbędna dla osiągnięcia celu ruchu trasa albo znika całkowicie, albo tworzy się pętla routingu (gdzie ruch jest przekazywany między dwoma routerami w nieskończoność) lub też ruch jest wysyłany do routera nieznającego trasy, w wyniku czego jest gubiony.

Nauczka?

W oparciu o to, co zostało powiedziane do tej pory, możliwe, że awaria Facebooka mogła, przynajmniej częściowo, być spowodowana błędną konfiguracją BGP.

Na tym etapie są to jednak zaledwie spekulacje i będziemy musieli poczekać, aż Facebook zdecyduje się powiedzieć, co tak naprawdę się działo i dlaczego. Niemniej, miniona awaria jest okazją, aby poświęcić nieco więcej uwagi tej mniej znanej, ale niezwykle ważnej części ruchu sieciowego. Pozwala ona przesyłać nie tylko wszystkie zabawne filmiki z kotami, ale także niezwykle istotne informacje biznesowe do naszych przeglądarek w całości i bez przeszkód.

Chmura nad Wisłą – tak, ale powoli.

Jak półtoraroczne doświadczenie pracy zdalnej rozbudziło świadomość i oczekiwania

Robert Paszkiewicz, odpowiedzialny w OVHcloud za region Europy Środkowo-Wschodniej

OVHcloud oraz Intel przyjrzały się rynkowi MŚP, sprawdzając stopień wykorzystania chmury. Badanie[1] wykazało, że podczas pandemii chmurą zainteresowało się 41 proc. firm, a 71 proc. planuje kolejne wdrożenia. Ankietowanych zapytano także o plany, motywacje i kryteria wyboru usług chmurowych oraz o to, jak decydenci oceniają praktyczne doświadczenia i modele realizacji wdrożeń.

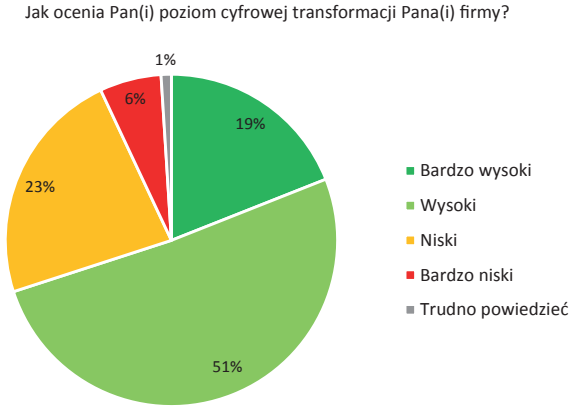
Okazuje się, że technologiczne zachmurzenie w Polsce postępuje konsekwentnie, lecz... nieśpiesznie. W przypadku firm z technologii chmury korzysta ponad połowa badanych (59 proc.), co świadczy o 7 proc. wzroście w porównaniu do 2020 r. Większe zastosowanie chmury deklarują przede wszystkim firmy, w których transformacja cyfrowa oceniana jest wysoko (65 proc.) i bardzo wysoko (74 proc.).

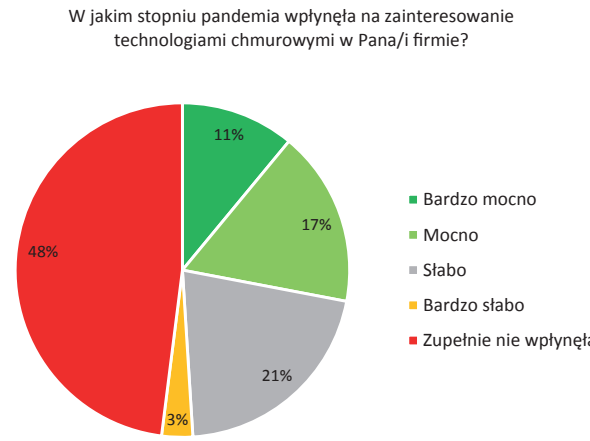
przedsiębiorstw. W niebyt, niezwykle szybko, poszły także obawy pracodawców o zmniejszoną produktywność zdalnych pracowników[2].

Jednak, jak wynika z badania, dopiero pełny rok pracy w nowej rzeczywistości pozwolił Polakom wygodnie rozsiąść się na „home office" i wyrobić sobie zdanie o oferowanych narzędziach. Obecnie transformację cyfrową wysoko lub lepiej ocenia już tylko 70 proc. ankietowanych, a nisko lub bardzo nisko aż 29 proc. (wcześniej tylko 9 proc.) Oczywiście to wciąż niezwykle dobry wynik. Zwłaszcza biorąc pod uwagę to, że podobny trend można zauważyć także w innych krajach. Również w Wielkiej Brytanii początkowo transformację cyfrową swoich firm pozytywnie oceniało aż 86 proc. pracowników. Obecnie już tylko 60 proc. ma nadzieję, że firmy zachowają nowe rozwiązania także po pandemii[3].

Rośnie świadomość deficytów

Z badań Eurostatu wynika, że obecnie z rozwiązań chmurowych w Polsce korzysta już co czwarta firma. To niemal podwójny wzrost w stosunku do wyników sprzed dwóch lat, gdy podobną deklarację składało jedynie 11 proc. Badanie przeprowadzone na zlecenie firm Intel i OVHcloud doprecyzowuje dodatkowo, że w aż 41 proc. badanych przedsiębiorstw pandemia wywołała wzrost zainteresowania wykorzystaniem chmury. Co istotne – przede wszystkim umacniając je w firmach, które już z niej korzystają. O kolejnym wdrożeniu myśli aż 71 proc. takich przedsiębiorstw. Natomiast spośród firm, które nie zdecydowały się

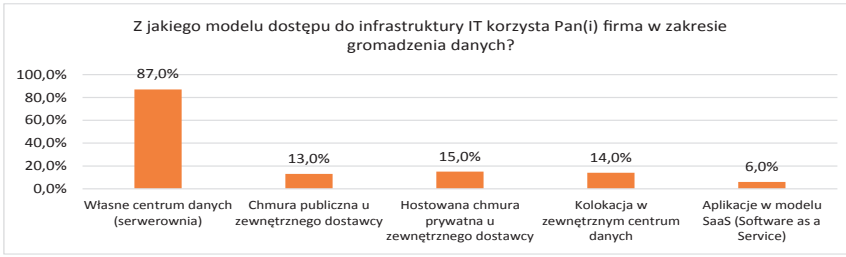




Badanie zrealizowane przez Data Tribe na zlecenie Intel i OVHcloud w X.2021 r.

Oczekiwania rosną z czasem

Po początkowym etapie chaosu oraz okresu ogromnego wzajemnego kredytu zaufania powiązanego z eksperymentami, jakie miały miejsce podczas pierwszych miesięcy pracy zdalnej, nastała faza zachwytu perspektywami. W 2020 roku aż 85 proc. badanych wysoko oceniało poziom transformacji cyfrowej swoich



Badanie zrealizowane przez Data Tribe na zlecenie Intel i OVHcloud w X.2021 r .

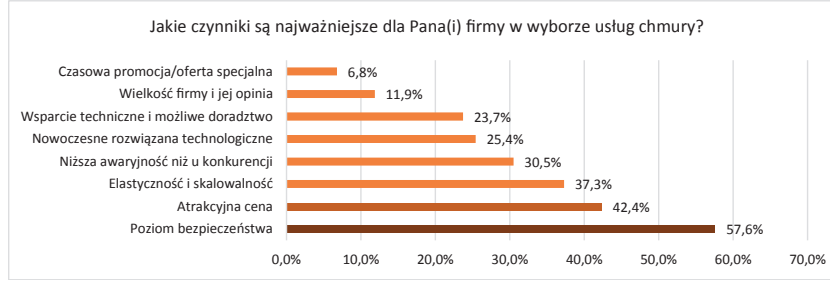
jeszcze na wdrożenie żadnych rozwiązań chmurowych, zastanawia się nad tym tylko 32 proc. Jednak co właściwie stoi na przeszkodzie?

Chmura opiera się przede wszystkim na zaufaniu. Firmom, które wykonały już pierwszy krok i przekonały się, ile wygody daje to rozwiązanie, łatwiej zdecydować się na następne. Prawie połowa użytkowników chmury zwraca uwagę przede wszystkim na wygodę, a więc brak konieczności budowania, utrzymywania czy chronienia własnej infrastruktury, pamiętając o okresowym zwiększonym zapotrzebowaniu na moc obliczeniową i zasoby pamięci.

Co stoi na przeszkodzie szybszego wzrostu popularności rozwiązań chmurowych w Polsce?

Czynnikiem hamującym decyzje o wejściu do chmury może być fakt, że własne serwerownie wciąż posiada aż 87 proc. badanych firm. Oczywiście własne zasoby nie przesądzają o braku możliwości skorzystania z chmury. Wiele firm zachowuje własną infrastrukturę w skali mikro z podstawowymi, kluczowymi zasobami, powierzając bardziej wymagające i ambitniejsze zadania dostawcom usług chmurowych. Warto też zauważyć, że tegoroczne 87 proc. to o 4 proc. mniej niż w roku 2020 r. Powoli więc zarysowuje się wyraźny trend. O ile bowiem wcześniej firmy zgłaszały, że temat chmury nie jest im do końca znany bądź obawiają się o bezpieczeństwo danych przechowywanych w chmurze (42 proc. w badaniu z 2020 roku), z najnowszych badań wynika, że kwestia bezpieczeństwa martwi już tylko co dziesiątą firmę (12 proc.).

Co więc powstrzymuje przesiadkę przedsiębiorców do chmury? Decydenci najczęściej wskazują brak konkretnej potrzeby (43 proc.). Można to tłumaczyć potrzebą wiedzy i przykładów efektów wdrożeń, jak chmura może pomóc w rozwoju. Na drugim miejscu znajduje się przekonanie, że posiadają już wystarczające zasoby wewnątrz własnej organizacji (22 proc.). Co ciekawe, koszty migracji wydają się odgrywać zupełnie drugorzędną rolę. Ten wątek wskazało już tylko 4,9 proc. firm.



Badanie zrealizowane przez Data Tribe na zlecenie Intel i OVHcloud w X.2021 r .

Jaką chmurę najchętniej wybierają polskie firmy i dlaczego?

Jak wynika z badania, duże firmy sięgają po chmurę prywatną znacznie częściej niż te średnie. Korzysta z niej już co piąta organizacja (21 proc.). Zdecydowana większość firm (aż 88 proc.) twierdzi, że przetwarza dane na serwerach zlokalizowanych w Polsce. Sama lokalizacja w Unii Europejskiej jest ważna dla 18 proc., czyli dla 5 proc. więcej niż w roku ubiegłym. Możemy więc mieć do czynienia ze wzrostem świadomości użytkowników. Tym bardziej, że serwery poza terenem Unii Europejskiej w dalszym ciągu nie cieszą się zaufaniem polskich firm. A potrzeba poczucia bezpieczeństwa była, podobnie jak w roku ubiegłym, najczęściej wskazywanym czynnikiem wyboru usług chmurowych (ma ona znaczenie aż dla 58 proc. respondentów).

Na kolejnym miejscu plasuje się natomiast atrakcyjna cena rozwiązań chmurowych, którą wskazało aż 42 proc. badanych. Warto jednak podkreślić, że nie chodzi o czasowe promocje. Te, jako czynnik zachęcający do rozpoczęcia podróży w chmurę, wskazało niespełna 7 proc. badanych, czyniąc je jednocześnie najrzadziej wskazywanym kryterium.

Na podium znalazła się także elastyczność, którą doceniło aż 37 proc. badanych firm. W tym przypadku też chyba najwyraźniej uwidocznił się wpływ pandemii. W tym roku wskazało na nią bowiem trzykrotnie więcej firm niż w 2020 r.

Wraz z elastycznością bezpieczeństwo staje się cechą wpisaną w usługi chmurowe. Upowszechnienie się modelu pracy zdalnej przyniosło nam natomiast niezwykle potrzebny wzrost świadomości i oczekiwań użytkowników. Wierzymy, że powoli będzie się to przekładać także na świadomość wszystkich zalet i zastosowań chmury.

[1] *Badanie zrealizowano w październiku 2021 r. przez Data Tribe. W ramach projektu zebrano dane z wykorzystaniem ilościowej metody badawczej wśród decydentów w zakresie IT na ogólnopolskiej próbie 100 firm zatrudniających 50 i więcej pracowników.*

[2] *https://www.rp.pl/rynek-pracy/art78481-pracodawcy-bardziej-podzieleni-w-ocenie-zdalnej-pracy-niz-pracownicy*

[3] *https://www.ukg.com/en-GB/about-us/newsroom/digital-transformation-dilemma-uk-employees-want-pandemic-era-tech-stay-says-research*

Łańcuch dostaw oprogramowania sposobem na cyberatak? Niestety coraz częściej tak. Jak się przed tym ustrzec?

W poszukiwaniu przewagi konkurencyjnej firmy coraz częściej korzystają z wyspecjalizowanych systemów oprogramowania. W efekcie posiadane przez nie zasoby IT stają się składanką systemów różnych dostawców. Może to zagrażać bezpieczeństwu informacji. Wraz ze wzrostem liczby rozwiązań rośnie liczba miejsc, które wymagają różnych form zabezpieczeń i uprawnień dostępowych. Sprawia to, że włamywacze mają do dyspozycji więcej potencjalnych punktów, przez które mogą próbować dostać się do zasobów firmy. Ponieważ w celu optymalizowania wydajności i produktywności firmy korzystają z coraz większej integracji systemów, atak może szybko się rozprzestrzenić.

Axel Simon,
open source security,
office of the CTO,
Red Hat

Ataki za pośrednictwem łańcucha dostaw oprogramowania — wykorzystujące oprogramowanie zewnętrznych dostawców w celu przeniknięcia do organizacji — stały się dziś praktycznie powszechne[1]. W 2020 r. szkodliwy kod wstrzyknięty w aktualizację oprogramowania firmy SolarWinds najpierw zaatakował departamenty rządu federalnego, a potem rozprzestrzenił się na skalę globalną, zarażając około 18 tys. organizacji. W marcu tego roku w związku z luką w oprogramowaniu Exchange Server firmy Microsoft naruszone zostały zabezpieczenia ponad 20 tys. amerykańskich organizacji. Nierzadko najwyższe ryzyko stwarzają pozornie mniej istotni partnerzy z łańcucha dostaw – ich rola nie wydaje się być znacząca, przez co nie dostrzega się w nich potencjalnego źródła zagrożenia. Jedno z największych naruszeń ochrony danych w historii to dokonany w 2013 r. atak na amerykańską sieć sklepów Target, zrealizowany poprzez włamanie do oprogramowania systemu klimatyzacji partnera tej firmy. Bezpieczeństwo łańcucha dostaw zyskało taką uwagę mediów, że stało się przedmiotem nowego rozporządzenia wykonawczego[2] prosto z Białego Domu.

Nie można zatem ignorować zagrożeń atakami opartymi na łańcuchu dostaw oprogramowania, jednak z drugiej strony na uwagę zasługują również obiecujące rozwiązania techniczne. Wiele organizacji musi pogodzić te dwie perspektywy. W praktyce może to zmuszać twórców oprogramowania do podjęcia decyzji: albo dokładamy starań, aby spełniać najwyższe standardy bezpieczeństwa, albo rezygnujemy z niedogodności i tarć, skupiając się na tworzeniu kodu.

Jednym ze sposobów pogodzenia tych pozornie przeciwstawnych trendów jest zmiana procesu podpisywania oprogramowania. Służy on zapewnieniu niepodważalnego dowodu, że przed wdrożeniem oprogramowanie nie zostało zmodyfikowane ani uszkodzone.

W tradycyjnych technikach podpisywania kodu stosuje się klucze kryptograficzne np. do weryfikacji autora i integralno-

ści zawartości repozytorium oprogramowania. Obciąża to programistów koniecznością generowania kluczy i przechowywania ich w bezpiecznym miejscu. Niektórym to obciążenie może wydawać się zbyt duże, więc przestają podpisywać swój kod (co jest szkodliwe z punktu widzenia zabezpieczeń) albo piszą go w mniejszej ilości (co nie służy innowacyjności). Oba podejścia niosą ze sobą konsekwencje dla innych programistów. Obecnie dużą część oprogramowania na świecie tworzy się na zasadach otwartego źródła, co oznacza, że każdy może taki kod wykorzystać i dostosować — w tej sytuacji kluczowe znaczenie ma kwestia pochodzenia. Dotyczy to w takim samym stopniu oprogramowania komercyjnego, które coraz częściej bazuje na publicznie dostępnym kodzie źródłowym.

A jednak to właśnie segment otwartego źródła zaczyna być liderem w tworzeniu coraz bardziej przyjaznego dla programistów środowiska podpisywania oprogramowania. Projekt ten nosi nazwę sigstore[3] i zastępuje klucze o długim czasie życia kluczami efemerycznymi powiązanymi z istniejącymi identyfikatorami (np. adresy e-mail i loginy do mediów społecznościowych). Generuje on także publiczny, niezmienny dziennik całej aktywności. Oba te elementy w gruncie rzeczy zdejmują z programistów obowiązek podpisywania oprogramowania, dzięki czemu mogą zająć się tym, w czym są najlepsi. Co więcej, system niebazujący na kluczach, które mogą zostać skradzione lub zgubione, jest z natury bezpieczniejszy.

Projekt błyskawicznie się rozwija. Od czasu jego uruchomienia w 2019 r. do jego twórców — firm Red Hat i Google oraz Uniwersytetu Purdue — dołączyły inne organizacje, a patronat nad projektem objęła Linux Foundation. Poszerzono także jego zakres, powołując do życia takie projekty pochodne jak Cosign (podpisywanie kontenerów i ogólnych artefaktów oprogramowania), Rekor (dziennik transparentności) i Fulcio (organ certyfikacji). Rozpoczęto także współpracę z innymi inicjatywami opartymi na otwartym źródle, m.in. z projektem Tekton Chains (pobocznym przedsięwzięciem w ramach projektu Tekton CI/CD).

To nie tylko ważne czynniki rokujące sukces. Wskazują one także możliwy sposób wdrażania projektu sigstore jako funkcji zintegrowanej w ramach szerszej technologii. Wszelkie działania zmierzające do wprowadzenia funkcji sigstore do istniejącego zestawu narzędzi programistów przybliżają osiągnięcie jednego z kluczowych celów projektu, jakim jest uproszczenie i zautomatyzowanie cyfrowego podpisywania, tak aby stało się częścią niewidzialnej infrastruktury, a programiści ani go nie zauważali, ani nie musieli się nim przejmować.

[1] *https://en.wikipedia.org/wiki/Supply_chain_attack*
[2] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/*
[3] *https://www.sigstore.dev/*

Niewielkie zasoby wodne w Polsce wymagają szczególnej ochrony, także z uwagi na zainteresowanie cyberprzestępców

Piotr Zielaskiewicz,
product manager
Stormshield

Aleksander Kostuch,
inżynier firmy
Stormshield

Zatrucie morskiej fauny i flory w efekcie przejęcia kontroli nad systemami oczyszczalni ścieków w Australii – tak przebiegał pierwszy cyberatak na instalacje wodne, od którego minęło 20 lat. Od tego momentu odnotowano liczne inne próby ataków na instalacje tego typu, a potencjalne konsekwencje wielu z nich, w tym skażenie wody pitnej, mogły dotknąć dziesiątki tysięcy ludzi. – Sektor wodno-kanalizacyjny pozostaje jednym z najbardziej krytycznych w strukturze państwa, przyciągając uwagę cyberprzestępców – wskazują eksperci Stormshield, wytwórcy rozwiązań w zakresie bezpieczeństwa sieci teleinformatycznych.

Opublikowane niedawno dane Głównego Urzędu Statystycznego[1] wskazują, że wielkość odnawialnych zasobów wody słodkiej na 1 mieszkańca Polski wynosi 1,6 tys. m3 (średnia z ostatnich 20 lat). To nie tylko jeden z najgorszych wyników w Europie, ale również wartość poniżej granicy uznawanej przez ONZ (1,7 tys. m3 na mieszkańca), wedle której kraj uznaje się za zagrożony niedoborem wody. Jednocześnie, jak pokazują dane hydrologiczne, miniony październik był miesiącem o rekordowo niskich opadach, miejscami tak niewielkich, jakich nie notowano w całej historii meteorologii. Dlatego zasoby wody pitnej wymagają szczególnej ochrony. Dodatkowo, jak wskazują eksperci Stormshield, sektor infrastruktury krytycznej, a w szczególności jego elementy odpowiadające za produkcję, dystrybucję i oczyszczanie wody, w coraz większym stopniu są narażone na działania cyberprzestępców. Wszystkie te czynniki czynią wodę dobrem wymagającym wielopłaszczyznowej ochrony.

Infrastruktura wodna jest sektorem krytycznym. Przestępcy mają wiele powodów, by go atakować, a uszkodzenie systemów informatycznych tego wrażliwego obszaru funkcjonowania państwa może mieć dramatyczne i dalekosiężne konsekwencje, w tym dla zdrowia, a nawet życia mieszkańców. Stąd nieustanna potrzeba dbałości o jak najlepsze zabezpieczenie przed niepożądanym dostępem do sieci.

Istotnym w tym kontekście zjawiskiem jest postępująca cyfryzacja branży. Przedsiębiorstwa wodociągowe coraz chętniej korzystają z rozwiązań cyfrowych, ale jednocześnie wciąż wiele z nich nie posiada w ogóle zabezpieczeń sieciowych. To powoduje, że stają się łatwiejszym celem dla cyberprzestępców. Przyczyny takiej sytuacji są różne, między innymi warto wskazać na niewielką świadomość zagrożenia czy brak wiedzy o zabezpieczeniach takich jak UTM/Next Generation Firewall przeznaczonych do ochrony sieci przemysłowych. Dodatkowym problemem jest brak środków finansowych czy wykwalifikowanej załogi, które są konieczne do wdrożenia skutecznych rozwiązań uniemożliwiających ataki. Wciąż mało powszechna jest także praktyka segmentacji sieci, czyli oddzielenia infrastruktury OT (sterowanie przemysłowe) od IT.

Zagrożenia są bardzo realne. Z jednej strony część przedsiębiorstw zupełnie nie korzysta z zabezpieczeń, a z drugiej wiele z firm wodociągowych czy stacji uzdatniania wody polega na wsparciu firm outsourcingowych, nadając im pełny, ale nieautoryzowany dostęp do całej swojej infrastruktury. Należy mieć świadomość swoich słabych punktów i na tej podstawie wprowadzać stosowne zabezpieczenia i procedury.

Problem został dostrzeżony przez władze centralne. Wiosną ubiegłego roku Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów wydał rekomendacje dla sektora wodno-kanalizacyjnego, wskazujące zagrożenia związane z wykorzystaniem infrastruktury IT/OT do ataków na sieci wodociągów i kanalizacji, oczyszczalnie ścieków i stacje uzdatniania wody.

W większości ataków, które były podstawą do wydania rekomendacji, zawiodło kilka elementów. Częstokroć wszystkie komputery bądź elementy produkcyjne systemu posiadały to samo hasło, a większość komputerów służących do zarządzania infrastrukturą była podłączona do internetu, choć nie posiadały firewalla. Z takich błędów mogą wyniknąć przykre konsekwencje. Kluczowe dla zwiększenia odpor-

ności infrastruktury jest zmniejszenie do minimum ekspozycji sieci przemysłowych do sieci publicznych, jak np. internet, czyli zastosowanie segmentacji. Obok wdrożenia rozwiązań typu UTM/Next Generation Firewall, przeznaczonych do ochrony sieci przemysłowych, należy dbać o dane uwierzytelniające, zmieniając je na trudne do złamania, a także ograniczać połączenia z siecią zewnętrzną jedynie do koniecznych z punktu widzenia monitorowania i zarządzania infrastrukturą.

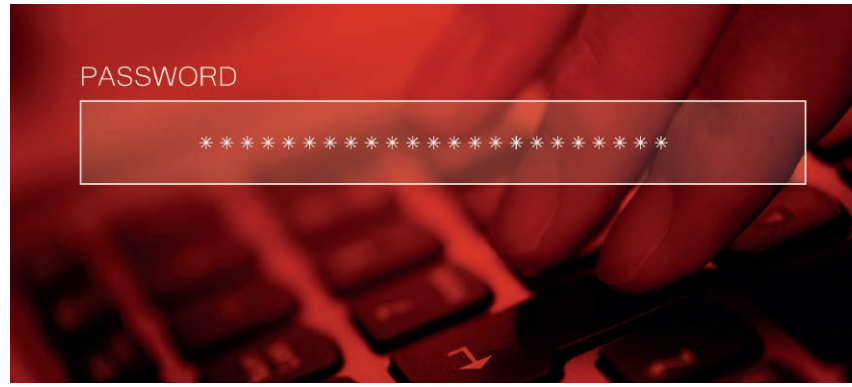
20 lat ataków na sektor wodny — przykłady

Oczyszczalnia ścieków w Shire of Maroochy w Australii w 2000 r.
W marcu i kwietniu 2000 r. były wykonawca techniczny oczyszczalni ścieków Maroochy w Australii przejął kontrolę nad jej systemami. Niedoszły pracownik, odrzucony w procesie rekrutacji, w ramach zemsty wysyłał fałszywe polecenia do systemów sterowania kilku pomp. W efekcie jego działań nastąpił wyciek ścieków do morza, co spowodowało zatrucie flory i fauny, a także pojawienie się nieprzyjemnego zapachu w okolicy.

Zakład wody pitnej w Georgii (Stany Zjednoczone) w 2013 r.
W kwietniu 2013 r. doszło do fizycznego ataku na obiekt dostarczający wodę pitną w małym miasteczku w jednym z amerykańskich stanów. Napastnicy po wejściu na teren instalacji uzyskali dostęp do systemu monitoringu, a następnie zmienili ustawienia fluoru i chloru, doprowadzając do zmiany składu chemicznego wody, z której korzystali mieszkańcy, co sprawiło, że przez kilka dni nie była ona zdatna do użytku.

Miasto Baltimore w Stanach Zjednoczonych w 20219 r.
Ataku typu ransomware w mieście Baltimore spowodował trzymiesięczne opóźnienia w wystawianiu rachunków za wodę.

Przepompownie i oczyszczalnie w Izraelu w 2020 r.
W kwietniu 2020 r. cyberprzestępcy, podejrzani o powiązania z irańskim reżimem, zaatakowali kilka przepompowni i oczyszczalnie ścieków oraz próbowali zwiększyć poziom chloru w systemach zaopatrzenia w wodę obsługujących część mieszkańców Izraela. Reakcją rządu na to zdarzenie było skłonienie pracowników całej infrastruktury wodnej i energetycznej do zmiany haseł do wszystkich swoich systemów SCADA, co miało chronić systemy przed dalszymi włamaniami.



Niemieckie firmy z sektora wodnego i przedsiębiorstwa energetyczne w 2020 r.
W 2020 roku rosyjska grupa Berserk Bear APT dokonała cyberataków na niemieckie firmy z przemysłową infrastrukturą krytyczną. Zakłada się, że była też wmieszana we wcześniejsze ataki cybernetyczne na niemieckie instalacje publiczne w 2018 roku.

Oczyszczalnie ścieków w San Francisco i na Florydzie (Stany Zjednoczone) w 2021 r.
W styczniu 2021 r. przejęto kontrolę nad zakładem uzdatniania wody w rejonie San Francisco, usuwając programy komputerowe związane z procesem uzdatniania wody pitnej. Wstępne wyniki śledztwa pokazują, że cyberprzestępca włamał się do systemów przy użyciu danych uwierzytelniających byłych pracowników, które zostały użyte do połączenia się z oprogramowaniem do zdalnego sterowania — TeamViewer.

W lutym 2021 r. miasto Oldsmar na Florydzie uniknęło katastrofy zdrowotnej, po tym jak cyberprzestępcy przejęli kontrolę nad miejską oczyszczalnią ścieków, której systemy komputerowe były niewystarczająco chronione. Również w tym przypadku kluczem dla cyberprzestępców były dane logowania do TeamViewera udostępnione przez kilku pracowników. Następnie próbowali wykorzystać oni luki w systemie operacyjnym Windows 7. Wtargnięcie pozwoliłoby znacznie zwiększyć poziom wodorotlenku sodu, czyniąc wodę pitną wyjątkowo toksyczną. Personelowi placówki udało się opanować sytuację i uratować około 15 tys. mieszkańców przed otruciem.

Infrastruktura uzdatniania wody w Norwegii w 2021 r.
Norweska firma Volue, która wyposaża zakłady uzdatniania wody w aplikacje i oprogramowanie, padła ofiarą oprogramowania ransomware o nazwie Ryuk. Szkodliwy program rozprzestrzenił się w systemach informatycznych dwustu publicznych dostawców wody w kraju, będących klientami firmy. Wedle niepotwierdzonych informacji szkodami zostało dotkniętych kilka platform klienckich. Volue szybko przedsięwzięła środki pozwalające na ograniczenie wpływu ataków, a następnie rozpoczęła przywracanie zainfekowanych systemów.

Obecnie wiele mówi się o wojnie hybrydowej, której celem jest destabilizowanie systemów krytycznych wrogiego Państwa i wzniecanie chaosu. Bronią, z której korzysta się w tego typu konfliktach, są cyberataki. Jak wykazuje analiza powyższych przykładów, metody ich prowadzenia są stale rozwijane. Ta broń jest intensywnie wykorzystywana, ponieważ zapewnia względną anonimowość sprawców. Z uwagi na obserwowane ostatnio intensyfikacje zagrożeń systemy zabezpieczeń w systemach wodno-kanalizacyjnych powinny być starannie zabezpieczone i monitorowane przez wykwalifikowanych specjalistów.

[1] *https://www.gov.pl/web/susza/najnowszy-raport-gus--polska-na-24-miejscu-w-unii-europejskiej-pod-wzgledem-odnawialnych-zasobow-wody-slodkiej*

Co zrobić, aby cyberprzestępczość była traktowana jak każdy inny rodzaj przestępczości, a hakerom nie opłacało się atakować?

Od kilku lat społeczna świadomość zagrożeń cybernetycznych rośnie. Wciąż jednak można usłyszeć, oczywiście poza branżą informatyczną, że cyberataki to po prostu „coś, co zdarza się w internecie". Nie każdy potrafi określić i porównać skutki ataków cybernetycznych. Jest to trudne zarówno w odniesieniu do osób, które padły ofiarą oszustw internetowych, jak i przedsiębiorstw zmuszonych do zapłacenia okupu w celu odzyskania dostępu do swoich systemów. Dlatego można odnieść wrażenie, że cyberprzestępczość nie zawsze jest postrzegana i traktowana jako „prawdziwa" przestępczość.

Dave Russell, wiceprezes ds. strategii korporacyjnej w firmie Veeam

Choć wiemy, że cyberprzestępstwo jest przestępstwem jak każde inne, niektórzy sobie tego nie uświadamiają. Trudno oczekiwać, aby ktoś poczuł się wstrząśnięty tym, iż jakiś haker przejął system międzynarodowej korporacji. Wynika to prawdopodobnie ze stereotypów przedstawiających cyberprzestępców jako młodych, zbuntowanych geniuszy informatyki, którzy „walczą z systemem", bo nie mają nic lepszego do roboty. Tymczasem za większością cyberataków stoją wielkie, zorganizowane i bogate organizacje przestępcze. Stosują one zaawansowane metody w celu okradania firm i instytucji publicznych, a to przecież okradane firmy i instytucje płacą nam wynagrodzenia czy świadczą codzienne, niezbędne usługi. Czy ktoś ma wątpliwości, że jest to przestępstwo?

Dlaczego obwiniane są ofiary?

Cyberprzestępstwo jest prawdziwym przestępstwem, a zaatakowane przez cyberprzestępców firmy są ofiarami. Ofiarami, które ponoszą straty na skutek popełnianych przeciwko nim czynów. Mimo to nasze współczucie wobec przedsiębiorstwa, które padło ofiarą ataku, jest nieporównanie mniejsze od tego, jakim gotowi jesteśmy obdarzyć pojedynczą, konkretną osobę. Gdy ktoś nam mówi, że hakerzy włamali mu się do systemu, przejęli dane osobowe i ukradli pieniądze, nigdy nie przyszłoby nam do głowy, aby go o to obwiniać. Jeśli jednak chodzi o firmy, to w następstwie cyberataków ponoszą one długotrwałe szkody na reputacji. W przypadku firm często zakładamy, że atak był spowodowany błędem lub brakiem ostrożności ofiary. Jako człowiek, który ma za sobą ponad 32 lata pracy w branży ochrony danych, nie mogę temu zaprzeczyć — zdecydowanej większości incydentów cybernetycznych da się uniknąć. Mają one miejsce dlatego, że firmy nie przestrzegają sprawdzonych procedur, nie dbają o higienę cyfrową, używają przestarzałego oprogramowania lub nie instalują poprawek zabezpieczających.

Nie ma chyba jednak drugiego takiego typu przestępczości, w przypadku którego wszyscy skupiają się niemal wyłącznie na obwinianiu ofiar zamiast na ściganiu sprawców. Zaatakowane firmy traktowane są raczej jak winowajcy, natomiast akceptuje się fakt, że przestępcy unikają kary na skutek braku globalnie uzgodnionych ram prawnych i odpowiedniego systemu sprawiedliwości. Przykładowo, jeśli przestępca z innego kraju przebywający w Stanach Zjednoczonych popełni przestępstwo przeciwko firmie mającej siedzibę w tym kraju, to istnieją procedu-

ry dyplomatyczne, które umożliwiają postawienie tego przestępcy przed sądem i zapewnienie ofierze odszkodowania. W przypadku ataku ransomware nie ma takich możliwości.

Jak stworzyć środowisko, w którym ryzyko dla cyberprzestępców jest większe niż zysk? Niezbędna jest w tym celu współpraca międzynarodowa i międzykontynentalna. Podczas pandemii plaga ataków ransomware nasiliła się, co zachęciło liderów sektora publicznego i biznesu do podjęcia działań w celu przełamania geopolitycznego impasu, który zapewniał cyberprzestępcom bezkarność. Nie będzie to jednak łatwe, a stworzenie całościowego, sprawnie działającego rozwiązania wymaga lat.

Nauczmy bronić się sami

Podczas gdy prawo nie zapewnia nam pełnej ochrony przed cyberprzestępczością, pierwotny ludzki instynkt przetrwania podpowiada, że powinniśmy bronić się sami. Wymaga to podjęcia kilku podstawowych kroków. Po pierwsze, każde przedsiębiorstwo powinno zatrudniać menedżera ds. bezpieczeństwa informatycznego, pracującego na miejscu, mającego zarówno stały kontakt z kierownictwem firmy, jak i uprawnienia do podejmowania inicjatyw w zakresie bezpieczeństwa. Osoba odpowiedzialna za cyberbezpieczeństwo i wyspecjalizowana w ochronie danych potrzebna jest również w mniejszych firmach. Po drugie, przedsiębiorstwa muszą bezwzględnie przestrzegać higieny cyfrowej. Dotyczy to w szczególności obowiązkowego szkolenia wszystkich pracowników w taki sposób, aby potrafili wykrywać potencjalne ataki, wiedzieli, komu je zgłaszać, i rozumieli, dlaczego jest to tak ważne. Im bardziej pracownicy będą się angażować we wdrażanie zasad higieny cyfrowej, tym większą będą mieć świadomość zagrożeń i skuteczniej im zapobiegać.

Na zakończenie jeszcze jedna rada: nigdy nie należy płacić okupu. Firmy, które płacą, dają cyberprzestępcom sygnał, że ataki ransomware to sposób na łatwe pieniądze, i zachęcają ich do kolejnych przestępczych działań. Gdy ofiary przestaną płacić, ataki ransomware staną się rzadsze, ponieważ stracą swoją skuteczność. Niezależnie od tego, że przedsiębiorstwa dotknięte cyberprzestępczością są ofiarami, mają one obowiązek ochrony wszelkich danych przez siebie używanych, przetwarzanych i przechowywanych. Płacenie cyberprzestępcom za przywrócenie dostępu do systemów nie może być traktowane jako strategia obrony, bo na dłuższą metę ona nie działa. Organy i instytucje rządowe podejmują coraz więcej działań, aby zapobiegać rozprzestrzenianiu się ataków ransomware. Firmy, które płacą okupy, mogą być ścigane i upominane przez niezależnych regulatorów.

Trzeba pamiętać, że mamy do czynienia z bezlitosnymi cyberprzestępcami, którzy działają na masową skalę, uderzając zarówno w firmy, jak i osoby prywatne. Walka z nimi wymaga podjęcia działań o zasięgu międzynarodowym, obejmujących sektor publiczny i prywatny. Nie ulega wątpliwości, że cyberprzestępczość powinna być traktowana jak każdy inny rodzaj przestępczości, a sprawcy ataków — ścigani i karani. Firmy muszą jednak pamiętać, że to one ponoszą odpowiedzialność wobec swoich klientów i pracowników za ochronę ich danych. Wszystkie te cele można osiągnąć tylko w jeden sposób — poprzez wdrożenie strategii nowoczesnej ochrony danych, która łączy efektywne zabezpieczenia cybernetyczne w obszarze interakcji z klientami z całościowym podejściem do tworzenia kopii zapasowych danych i przywracania systemu po awarii.

Jak przetestować plan usuwania skutków katastrofy, a przy okazji cały zespół

Plany usuwania skutków katastrofy (Disaster Recovery — DR) są dziś centralnymi mechanizmami ochrony środowisk informatycznych przedsiębiorstw przed różnego rodzaju zagrożeniami, od ataków hakerskich po klęski żywiołowe. W sytuacji gdy ataku ransomware spodziewa się 6 na 10 firm, które dotąd go nie doświadczyły, a ponad połowa z nich (54%) wskazuje, że cyberataki są obecnie zbyt zaawansowane, aby je zatrzymać, niezwykle ważne staje się testowanie planów DR . Niestety, nie jest to powszechna praktyka. Specjaliści w centrach przetwarzania danych są tak przeciążeni pracą, że nie mają ani czasu, ani narzędzi, aby przeprowadzać takie testy częściej.

Rick Vanover, dyrektor ds. strategii produktowej w firmie Veeam

Testowanie planów DR ma ogromne znaczenie, ponieważ szybkie przywrócenie normalnego funkcjonowania środowiska informatycznego zależy nie tylko od procedur, lecz również od koordynacji, współpracy i odpowiedniej kolejności działań w zespole realizującym taki plan. Niezbędne są też odpowiednie struktury obejmujące pamięć masową, sieć, aplikacje, bazy danych i inne zdalne platformy robocze.

Cyberataki mogą poważnie zmniejszyć produktywność firmy i jej zdolność do szybkiego odzyskiwania danych, ale istnieje też inne — dużo bardziej prawdopodobne, choć często niedostrzegane —zagrożenie: błędy spowodowane nieumyślnie przez człowieka. W niektórych krajach odsetek takich incydentów osiągnął poziom aż 38%. Oprogramowanie do automatycznego wykrywania zagrożeń może pomóc w wykrywaniu nieprawidłowych zachowań i innych oznak włamania do środowiska informatycznego. Zawsze

jednak pierwszą linię obrony stanowią pracownicy firmy.

Czym jest plan usuwania skutków katastrofy (DR)?

Veeam definiuje plan DR jako zestaw procedur , które należy wykonać w przypadku nieplanowanego zdarzenia zakłócającego pracę zasobów przedsiębiorstwa oraz narażającego na ryzyko bieżące procesy i operacje. Katastrofy mogą mieć różne rozmiary, przyczyny i formy, takie jak klęski żywiołowe, awarie sprzętu, cyberataki lub błędy człowieka.

Planowanie pomaga firmie w znalezieniu najlepszej strategii walki z takimi zagrożeniami oraz ograniczeniu do minimum wynikających z nich przestojów. W czasie, gdy liczba wektorów ataków cały czas rośnie, plany DR są niezbędne dla zapewnienia ciągłości działania firmy.

Ludzka strona technologii

Nie da się zaprzeczyć, że błąd człowieka może doprowadzić do utraty danych, każda firma musi więc zachować czujność i szkolić swoich pracowników w zakresie przeciwdziałania takim incydentom. Jak wskazano w opublikowanym niedawno raporcie firmy PC World, przyczyną 75% przypadków utraty danych były błędy człowieka .

Z kolei katastrofy cybernetyczne następują najczęściej z takich przyczyn jak błędy podczas wysyłania wiadomości e-mail, przypadkowe usunięcie danych, niedostateczna higiena informatyczna, uszkodzenie danych oraz brak szkoleń pracowników w zakresie aktualnych zagrożeń. Co łączy wszystkie te incydenty? Otóż ich skutki można z powodzeniem ograniczyć za pomocą środków takich jak odpowiednie szkolenia pracowników, stosowanie rygorystycznych zasad wewnętrznych oraz szersze i dokładniejsze analizowanie współczesnych zagrożeń.

Zapobieganie utracie danych w wyniku błędu człowieka

Przeciwdziałanie błędom człowieka nie powinno mieć charakteru reaktywnego. Wskazane są środki proaktywne, które w razie takiego incydentu umożliwią szybką reakcję i ograniczenie strat do minimum. Przykładami skutecznych działań są szkolenia pracowników, wdrożenie odpowiednich reguł wewnętrznych i właściwe zaprojektowanie zadań.

Problemem jest także fakt, że bardzo często to właśnie menedżerowie nie przywiązują należytej wagi do dobrych praktyk i szkoleń w zakresie bezpieczeństwa. Niezależnie od tego, czy takie praktyki i szkolenia stanowią część kompleksowej strategii bezpieczeństwa informatycznego, czy też są organizowane odrębnie, firmy powinny szkolić wszystkich swoich pracowników w zakresie bezpiecznych procedur podczas pracy w trybie online. Dotyczy to w szczególności osób pracujących zdalnie. Może to znacznie zmniejszyć ryzyko utraty danych spowodowanej przez ataki ransomware lub inne formy szkodliwego oprogramowania.

Z jednej strony należy szkolić w zakresie cyberbezpieczeństwa pracowników niebędących informatykami, z drugiej jednak równie ważne jest regularne szkolenie i podnoszenie kwalifikacji personelu działu informatycznego. Informatycy odgrywają kluczową rolę w realizacji planu DR oraz zapewnieniu dostępności systemu w sytuacjach awaryjnych, a wdrożenie wydajnego i skutecznego planu DR wymaga dobrej znajomości i dogłębnej analizy istniejących zagrożeń.

Pracownicy powinni znać i rozumieć stosowane w przedsiębiorstwie najlepsze procedury dotyczące cyberbezpieczeństwa, takie jak ograniczenie dostępu do plików, stosowanie silnych haseł i uwierzytelniania, propagowanie dobrych nawyków dotyczących tworzenia kopii zapasowych, używanie bezpiecznej sieci i rutynowe kontrole higieny cybernetycznej. Wszystko to w połączeniu z odpowiednią strategią informatyczną znacznie zmniejsza ryzyko incydentów spowodowanych błędem człowieka.

Najważniejszy jest człowiek

Choć testy planów DR są bardzo ważne ze względu na swój cel, obejmują one tylko aspekt techniczny. Jeśli dojdzie do faktycznej katastrofy, pracownicy muszą działać szybko i profesjonalnie, aby przywrócić działanie środowiska informatycznego. Przeprowadzenie testów fizycznych i symulacyjnych pomoże przygotować zespół do działania w sposób zgodny z zasadami i procedurami firmy. W tym przypadku nie ma miejsca na podziały czy też przeciwstawianie myślenia indywidualnego myśleniu zespołowemu.

Należy zawsze pamiętać, że w przypadku katastrofy najważniejszym zasobem firmy są jej pracownicy. Warto więc poświęcić czas i wysiłek na ich odpowiednie przeszkolenie. Od tego może zależeć, czy firma przetrwa i będzie nadal odnosić sukcesy.

Ransomware – szybsze, trudniejsze do wykrycia i bardziej szkodliwe

Przewodnik po nowoczesnej obronie

Ireneusz Wiśniewski,
dyrektor zarządzający
F5 Poland

Ataki ransomware stały się ciężarem finansowym i poważnym zagrożeniem dla infrastruktury o krytycznym znaczeniu. Nowoczesne oprogramowanie tego typu sprawdza, gdzie jest, może się usunąć, ukryć, uśpić lub samoistnie zniszczyć. Omija filtry narzędzi antywirusowych i wyłącza narzędzia obrony. Samodzielnie się szyfruje i rozpakowuje. Używa także narzędzi i funkcji systemu Windows do własnych potrzeb skanowania.

Szybsze tempo

Oprogramowanie mające wyłudzić okup działa błyskawicznie. Dzieje się tak, ponieważ może ono pozostawać w stanie uśpionym, sondując otoczenie w poszukiwaniu najlepszego miejsca do ataku. W tym czasie hakerzy uszkadzają punkty odtwarzania kopii zapasowej i usuwają zawartość koszy, aby udaremnić działania zaradcze. Następnie uruchamiany jest atak i szyfrowanie wszystkich zasobów naraz. Ransomware może także szybciej rozprzestrzeniać się z dobrze skomunikowanych wewnętrznych węzłów sieci (takich jak kontrolery domen w systemie Windows), które prowadzą interakcję z większością systemów wewnętrznych.

Trudniejsze wykrycie

Uśpione ransomware omija filtry narzędzi antywirusowych, które oczekują, że szkodliwe oprogramowanie uruchomi się natychmiast. Większość takich nowoczesnych programów wyłącza narzędzia antywirusowe lub ukrywa się, samodzielnie szyfruje, rozpakowując się wyłącznie w pamięci, tak aby ominąć narzędzia skanujące dyski[1]. Oryginalny plik, który zostanie załadowany do pamięci i zaszyfrowany, zastępują na kilka sposobów: zamieniając w nim dane, podmieniając pod starą nazwą czy nadpisując.

Nowsze odmiany ransomware omijają Microsoft Defender, korzystając z maskowania RIPlace i używając starszej funkcji systemu Windows, dzięki której mechanizm zmiany nazwy i nadpisywania plików może działać w sposób niewykrywalny, obchodząc w ten sposób kontrolowany dostęp do folderów.

Nowe warianty potrafią też ukryć obniżenie wydajności systemu powodowane szyfrowaniem, wyświetlając fałszywe komunikaty o błędach. Ponadto wykorzystują wbudowane narzędzia i funkcje sys-

temu Windows na potrzeby skanowania i wybierania celów.

Inteligentniejsze ransomware

Kiedyś wystarczyło zbadać pliki binarne atakującego programu, które czasami zawierały klucz szyfrowania, lub przekazać informację o wykrytym ransomware[2] do działu analizy zagrożeń, aby opracować nowe mechanizmy ochrony.

Odpowiedzią hakerów było opracowanie szkodliwego oprogramowania ulegającego samozniszczeniu. Gdy usługa wykonująca program przestaje działać, powoduje awarię uniemożliwiającą odczytanie pamięci. Oprogramowanie ransomware nie uruchomi się, jeśli wykryje swoją obecność w środowisku wirtualnym lub debugerze, a jego kod może wówczas wprowadzić w błąd narzędzia analityczne. Ponadto niektóre warianty aktywują się dopiero wtedy, gdy haker wyśle kod odblokowujący, co utrudnia mechanizmom obrony przechwycenie i przeanalizowanie szkodliwego programu.

Jak zatrzymać udoskonalone ransomware

Bez względu na poziom zaawansowania kodu program infekujący musi dostać się do systemów firmy. W tym celu stosuje techniki phishingu, uzyskuje nieautoryzowany dostęp, a także wykorzystuje znane luki w zabezpieczeniach.

Dlatego:

- Zbadaj i zinwentaryzuj powierzchnię ataku[3], aby zrozumieć, gdzie występują zagrożenia.
- Odszyfruj, zbadaj i zablokuj elementy pobrane przez użytkowników oraz ruch pocztowy.
- Wprowadź mechanizmy silnego uwierzytelniania[4].
- Przejrzyj zabezpieczenia stosowane przez podmioty spoza firmy[5], ogranicz prawa ich dostępu.
- Usuń luki w zabezpieczeniach, najpierw te dot. wykorzystywanych eksploitów[6].

Gdy oprogramowanie ransomware dostanie się już do systemów, trzeba skonfigurować mechanizmy tzw. obrony w głąb[7]; wzmocnić zabezpieczenia kontrolerów domen i zastosować w nich poprawki. Jeśli hakerzy będą próbowali wykorzystywać zasoby naturalne, trzeba ograniczyć dostęp do narzędzi takich jak PowerShell, Nltest, PsExec, McpCmdRun i WMic za pomocą zasad grup.

Warto ograniczyć otwarte współużytkowanie wewnętrznych plików. Zainfekowanie jednego urządzenia oznacza, że wszystkie współużytkowane pliki zostaną zaszyfrowane i/lub wycieknią. Należy też usuwać lub wyłączać nieaktualne wersje łatwego do pokonania przez ransomware protokołu Server Message Block (SMB).

Ograniczanie szkodliwości oprogramowania ransomware

Oprogramowanie ransomware może wydobyć terabajty danych, więc należy ograniczyć lub objąć monitoringiem ruch wychodzący. Oznacza to konieczność użycia narzędzi m.in. do odszyfrowywania i badania ruchu SSL dla wczesnego rozpoznania ataku. Konieczne jest tworzenie kopii zapasowej systemów i danych krytycznych przechowywanej poza siecią oraz utworzenie szablonów, dzięki którym systemy będzie można szybko zrekonfigurować od podstaw.

Jeśli jednak dojdzie do zainfekowana oprogramowaniem ransomware, pozostaje skontaktowanie się z organami ścigania. Dzięki temu firma w mniejszym stopniu naraża się na ewentualne naruszenie przepisów, jeśli postanowi zapłacić przestępcom. Nawet jeśli organizacja zdecyduje się zapłacić okup, należy odbudować wszystkie systemy, których zabezpieczenia mogły zostać naruszone, tak aby mieć pewność, że zostały one oczyszczone ze szkodliwego oprogramowania.

1 *https://oxoo-oxoo.github.io/research/2018/10/28/How-to-bypass-AMSI-and-Execute-ANY-malicious-powershell-code.html*

2 *https://www.f5.com/labs/articles/threat-intelligence/from-ddos-to-server-ransomware-apache-struts-2-cve-2017-5638-campaign-25922*

3 *https://www.f5.com/labs/articles/bylines/to-protect-your-network-you-must-first-know-your-network*

4 *https://www.f5.com/labs/articles/cisotociso/tips-and-tricks-for-rolling-out-multi-factor-authentication*

5 *https://www.f5.com/labs/articles/cisotociso/third-party-security-is-your-security*

6 *https://www.f5.com/labs/articles/cisotociso/prioritizing-vulnerability-management-using-machine-learning*

7 *https://www.f5.com/labs/articles/cisotociso/build-defense-in-depth-with-dissimilar-protections*

Jak kształcić nowe pokolenie specjalistów ds. cyberbezpieczeństwa

Ważnym elementem Europejskiego Miesiąca Cyberbezpieczeństwa jest dyskusja na temat luki kompetencyjnej w branży. O tym, jak kształtować nowe pokolenie specjalistów i jakie umiejętności są im potrzebne, mówi w rozmowie z przedstawicielami Fortinet Jeff Robbins, Practice Director w Business Communications, Inc.

Czy możesz opisać obecny stan branży cyberbezpieczeństwa?

W ciągu ostatnich 10 lat charakter zagrożeń naprawdę się zmienił. Obecnie mamy do czynienia ze skutecznymi i zaawansowanymi technicznie cyberprzestępcami — nie tylko uruchamiają oni skrypty, ale dysponują wyrafinowanymi narzędziami. Nie wszyscy spoza naszej branży rozumieją poziom umiejętności, które są potrzebne, aby przeciwdziałać cyberprzestępczości.

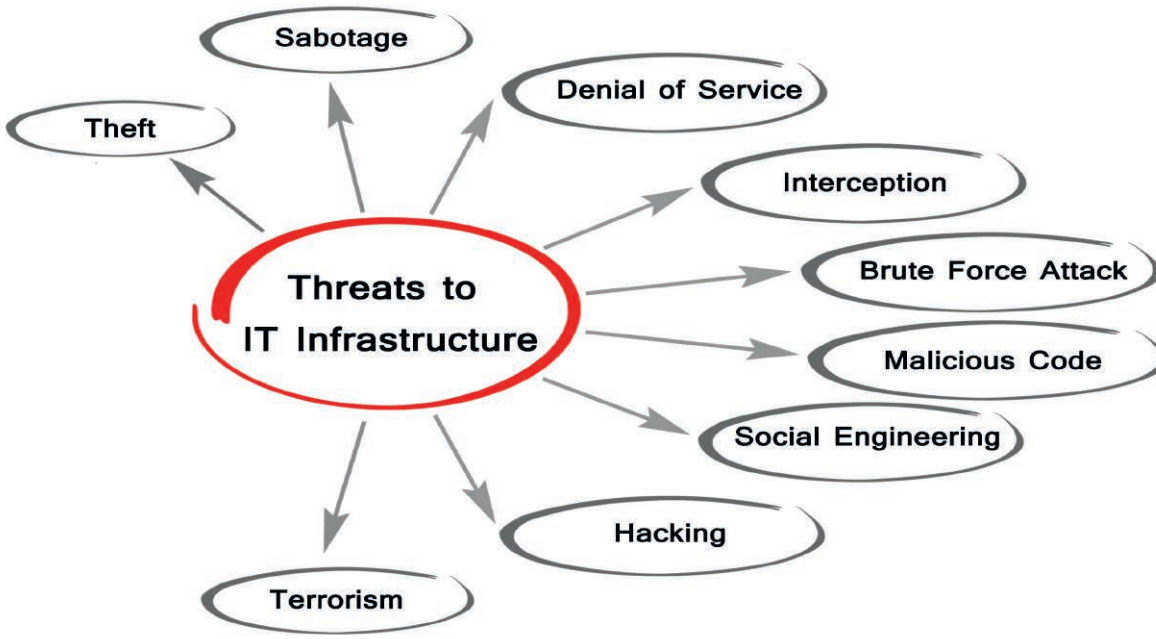
Cyberprzestępcy są też bardzo zmotywowani z powodu pieniędzy, które mogą zarobić. Dobrze znane ataki sponsorowane przez rządy są tylko jednym z wielu przykładów. Większość z nas na co dzień ma do czynienia z nowym, zupełnie innym poziomem przestępczości niż 10 lat temu. Hakerzy są sprytni, żądni pieniędzy, uzdolnieni technicznie, a ich działania są połączone w ramach jednego ekosystemu. Nic więc dziwnego, że cały czas widzimy statystyki dotyczące wzrostu poziomu cyberprzestępczości oraz liczby cyberataków.

Co według ciebie jest obecnie najlepszą obroną przed cyberprzestępczością?

Uważam, że bardzo ważne jest posiadanie silnego wewnętrznego procesu zarządzania, oceny ryzyka i zgodności procedur z prawem. Problemem, który często obserwuję, jest to, że choć wiele firm ma i politykę, i procedury, które dyktują, jak wszystko powinno działać, to często brakuje im odpowiednio przeszkolonych pracowników, którzy mogliby te zasady wdrożyć. Dlatego tak ważne jest posiadanie odpowiednio przeszkolonego personelu na poziomie eksperckim w zakresie technicznych mechanizmów kontroli, które są stosowane w danym środowisku.

Jak możemy zlikwidować lukę w umiejętnościach w zakresie cyberbezpieczeństwa?

Łatwiej powiedzieć niż zrobić, ale w tym celu należy zatrudnić więcej ludzi! Nie



mamy innego wyboru, jak tylko rozwijać talenty wewnątrz firmy. W idealnej sytuacji szukamy ludzi, którzy zaangażują się w proces zdefiniowany w celu rozwijania talentów. Średni staż pracy naszych inżynierów bezpieczeństwa wynosi ponad 10 lat, co jest świetnym wynikiem, ale musimy również zatrudniać nowe pokolenie specjalistów, którzy przejmą pałeczkę. Naszym wyzwaniem jest znalezienie następnej generacji utalentowanych pracowników. Podnoszenie kwalifikacji od wewnątrz poprzez praktyczne doświadczenie i programy certyfikacji jest niezbędne, ale niełatwe – wymaga czasu i inwestycji. Lubię powtarzać mojemu zespołowi, że o 17.00 chcemy być lepsi niż o 8.00 rano, a każda interakcja z mniej doświadczonymi inżynierami powinna mieć charakter edukacyjny.

Jaką wartość przywiązujecie do certyfikacji?

W naszej branży musimy wyróżniać się najlepszymi inżynierami. A sposobem, w jaki to udowadniamy, są certyfikaty. Pokazują one naszym klientom, że nasz zespół jest wartościowy i że jesteśmy dobrzy w tym, co robimy. Na przykład, mamy kilku specjalistów certyfikowanych na poziomie NSE 8, ale chciałbym mieć ich znacznie więcej. Muszę tylko znaleźć trochę czasu dla naszych pracowników, aby mogli przystąpić do egzaminów. Biorąc pod uwagę ich doświadczenie techniczne i branżowe, wiem, że są gotowi, co jest obiecujące, biorąc pod uwagę istniejącą lukę kompetencyjną.

Co oznacza dla ciebie posiadanie certyfikatu NSE 8?

Daję przykład i jednocześnie chcę wyróżnić naszych inżynierów spośród innych oraz wskazać odpowiednią ścieżkę kariery. Posiadanie certyfikatu poziomu 8 pokazuje naszym klientom, że mamy najlepszych ekspertów w branży. Certyfikacja udowadnia, że jesteśmy w pełni zaangażowani w swojej działalności. Zaprezentowanie dogłębnej wiedzy na temat rozwiązań technicznych jest ważne dla klientów, gdy mówimy o tak ważnym obszarze jak cyberbezpieczeństwo.

Jakich umiejętności poszukujecie u pracowników?

W dzisiejszych czasach trudno jest zatrudnić najlepszych, ponieważ jest ich niewielu i są naprawdę drodzy. Muszę więc skupić się na inżynierach mających certyfikację na poziomach 1 i 2, którzy są chętni do nauki i rozwoju. Bardziej niż umiejętności szukam zainteresowania i głodu wiedzy, a także ludzi, którzy mają talent do jej szybkiego przyswajania i uczenia się w trakcie pracy. Zawsze szukamy ludzi, którzy chcą coś zmienić i chcą zajmować się cyberbezpieczeństwem. Nie jest to łatwa praca, trzeba naprawdę chcieć być częścią tej dziedziny. Jest to również powód, dla którego szkolenia i certyfikaty z zakresu bezpieczeństwa cybernetycznego są tak wartościowe. Mogą pomóc w rozwoju talentu i dać możliwości zrobienia kariery tym, którzy chcą się uczyć i zainwestować swój czas w rozwój.

Jeff Robbins *posiada certyfikat Network Security Expert (NSE) na najwyższym poziomie 8 w ramach programu certyfikacji NSE, prowadzonego przez Fortinet Training Institute. Aby osiągnąć ten poziom, dana osoba musi mieć znaczne doświadczenie w branży oraz wykazać się biegłością w obsłudze rozwiązań Fortinet poprzez zdanie zarówno*

Jak świat walczy z cyberprzestępczością? Globalne sojusze i dzielenie się wiedzą

Derek Manky,
FortiGuard Labs

Współczesne cyberzagrożenia stają się coraz bardziej wyrafinowane, a prowadzenie ataków typu ransomware przenoszone jest na model bazujący na sieciach afiliacyjnych i usługach. Przestępcy wiedzą, że ich biznes wart jest biliony dolarów, a jednocześnie szanse na złapanie przez policję są dość niskie, ponieważ siatki cyberprzestępcze rozciągają się ponad granicami państw. W takiej sytuacji ich zwalczanie to wspólny wysiłek ekspertów ds. bezpieczeństwa, organów ścigania, rządów, biznesu i całego społeczeństwa.

Igła w stogu siana

Cyberprzestępczość to obecnie imperium, które funkcjonuje jak każda inna organizacja przestępcza tego rodzaju – z szefami, menedżerami i słupami. Jej świat jest jednak nieco bardziej skomplikowany. Weźmy na przykład najważniejszy powód, dla którego hakerzy nie dają się złapać – jest to jurysdykcja. Wielu cyberprzestępców działa w krajach, które nie mają podpisanej umowy o ekstradycji, np. do Stanów Zjednoczonych. Utrudnia to ich namierzenie, pojmanie i postawienie w stan oskarżenia.

Istnieje mnóstwo danych na temat oprogramowania ransomware i innych rodzajów cyberprzestępczości. Jednak dokładne oszacowanie skali tego zjawiska jest trudne, ponieważ znaczna część ofiar nie zgłasza się do organów ścigania. Mimo że ostatnio odnotowano kilka dużych udanych ataków, to wciąż mniej niż 0,05% cyberprzestępców zostaje aresztowanych i postawionych przed sądem. Daje to przestępcom poczucie pewności siebie i pozwala im działać bez obaw, że poniosą konsekwencje. Łańcuch dostaw cyberprzestępczości rozrósł się, a w każdym jego punkcie znajduje się tak wiele ruchomych części oraz uczestników, że potrzeba wspólnych, globalnych wysiłków, aby ich wszystkich wytropić i powstrzymać.

2021 rokiem zmian

W cyberbezpieczeństwie nie każde działanie ma natychmiastowy lub trwały efekt. Jednak kilka wydarzeń, jakie miały miejsce w 2021 roku, wskazuje na zacho-

dzące pozytywne zmiany w walce przeciwko przestępcom.

Połączenie sił poprzez współpracę jest traktowane jako działanie priorytetowe, które ma na celu przerwanie łańcuchów dostaw cyberprzestępców. Dzielenie się danymi oraz nawiązane partnerstwa umożliwiają skuteczniejsze reagowanie na działania hakerów i lepsze przewidywanie, z jakich technik będą korzystali w przyszłości. Wyniki tej współpracy to np. skoordynowane przejęcie infrastruktury Emotetu, jednego z najskuteczniejszych szkodliwych narzędzi w ostatnich latach oraz przerwanie kampanii ransomware Egregor, NetWalker i Clop. Są to poważne sukcesy rządów i organów ścigania w walce z cyberprzestępczością. Amerykański Departament Sprawiedliwości postawił nawet w stan oskarżenia osobę powiązaną z NetWalkerem. Dane FortiGuard Labs wykazały spowolnienie aktywności szkodliwych narzędzi po wyeliminowaniu Emoteta. Z kolei aktywność związana z wariantami TrickBot i Ryuk utrzymywała się po tym wydarzeniu, jednak jej skala była mniejsza.

Wspólny wysiłek

Misją FortiGuard Labs jest dostarczanie klientom Fortinet najlepszych informacji o zagrożeniach, aby chronić ich przed szkodliwą działalnością i wyrafinowanymi cyberatakami. Nie poprzestajemy jednak na tym. Fortinet aktywnie współpracuje z ponad 200 partnerami, z którymi wymienia się informacjami o zagrożeniach. Należą do nich firmy zajmujące się wywiadem w zakresie cyberzagrożeń, krajowe zespoły reagowania kryzysowego CERT, zespoły reagowania na incydenty bezpieczeństwa komputerowego CSIRT, agencje rządowe, organizacje międzynarodowe, w tym NATO i Interpol, oraz inni kluczowi partnerzy, tacy jak MITRE i Centrum Cyberbezpieczeństwa Światowego Forum Ekonomicznego.

Fortinet należy również do działającej w strukturach Interpolu Globalnej Grupy Ekspertów (ICGEG), a także współpracuje z agencją FBI, której pomaga w zwalczaniu cyberprzestępczości i cyberterroryzmu. Jest jedną z kilku firm z sektora prywatnego, które udzieliły wsparcia operacji prowadzonej przez Interpol, mającej na celu zwalczanie cyberprzestępczości w regionie ASEAN. Fortinet jest też współzałożycielem organizacji Cyber Threat Alliance (CTA). Rozrosła się ona z czterech członków założycieli do aktywnie działającego zrzeszenia badaczy zagrożeń, dostawców zabezpieczeń i partnerów sojuszu w celu wymiany informacji o zagrożeniach i usprawnienia obrony przed cyberprzestępczością w firmach członkowskich i u ich klientów. Celem CTA jest uniemożliwienie przeprowadzania ataków poprzez zwiększenie poziomu cyfrowej odporności – im bardziej podmioty dzielą się wiedzą, tym lepiej będą przygotowane do walki z cyberprzestępczością.

Fortinet jest również członkiem-założycielem i wspiera wiele inicjatyw Centrum Bezpieczeństwa Cybernetycznego Światowego Forum Ekonomicznego – zajmuje jedno z zaledwie dwóch stałych miejsc w tej międzynarodowej radzie. Centrum Bezpieczeństwa Cybernetycznego zostało stworzone, aby kształtować przyszłość tej dziedziny, budować zaufanie cyfrowe na całym świecie, chronić innowacje, instytucje, firmy i osoby prywatne oraz zabezpieczać nasze rosnące uzależnienie od gospodarki cyfrowej.

Branża handlowa najbardziej dotknięta przez ransomware – badanie Sophos

Grzegorz Nocoń,
inżynier systemowy
w firmie Sophos

Branża handlowa najczęściej ze wszystkich doświadcza ataków ransomware. Według analizy ekspertów firmy Sophos aż 44% należących do niej firm doświadczyło w ostatnim roku cyberataku, w którym przestępcy zaszyfrowali dane i żądali okupu za ich odblokowanie. Koszty związane z obsługą tych zdarzeń, w tym przestoje, naprawa systemów IT czy odpływ klientów, wynosiły średnio prawie 2 mln dolarów. Obecnie trwa najbardziej „gorący" okres zakupowy w roku, a dane klientów to cenna waluta dla przestępców. Co mogą zrobić sklepy i konsumenci, żeby je chronić?

Sklepy atrakcyjnym celem dla przestępców

Firmy z branży handlowej przechowują wiele poufnych danych osobowych klientów. Cyberprzestępcy mogą sprzedać je na czarnym rynku lub wykorzystać w kolejnych atakach. Pandemia i sezon świąteczny dodatkowo ułatwiają atakującym zadanie – skokowo wzrasta liczba transakcji online i ruch na stronach internetowych sklepów, co dokłada pracy zespołom IT. Wiele placówek handlowych korzysta ze starszych i rozproszonych systemów, trudnych w aktualizacji, co dodatkowo utrudnia ochronę zasobów. Prawie 2/3 firm z branży, które nie doświadczyły ataku ransomware w ubiegłym roku, spodziewa się go w przyszłości.

Podmioty handlowe są szczególnie atrakcyjnym celem cyberataków, gdyż przetwarzają wiele danych, takich jak numery kart płatniczych, adresy e-mail, telefony czy daty urodzenia. Dlatego każdy sklep powinien priorytetowo traktować kwestie cyberbezpieczeństwa i inwestować w rozwiązania ochronne, które zablokują ataki. Nie mniej istotne jest szkolenie pracowników, regularne tworzenie kopii zapasowych i plan szybkiego reagowania na incydenty, który pomoże szybko wznowić działalność i minimalizować straty.

Wysokie koszty ataków dla firm i klientów

Prawie połowa placówek handlowych doświadczyła ataku ransomware w ostatnim roku. W 54% przypadków przestępcom udało się zaszyfrować dane. Co trzecia firma, której dane zablokowano, zapłaciła okup – średnio 147 811 dolarów. Branża handlowa odnotowała też więcej ataków, w których dane zostały wykradzione pod groźbą ujawnienia, niż inne branże (12% w porównaniu ze średnią 7% dla wszystkich branży).

Firmy handlowe ponoszą też wysokie koszty postępowania w przypadku naruszenia danych. Muszą powiadomić wszystkich, których dane wyciekły bądź zostały trwale zablokowane, oraz przebudować i zabezpieczyć systemy informatyczne. Straty wynikają również z przestojów w działalności, utraconej reputacji i odpływu klientów – znacznie łatwiej jest im zmienić sklep internetowy niż szkołę czy dostawcę energii.

Co może zrobić klient?

Cyberatak oznacza ryzyko dla sklepu i jego systemów IT, ale też dla klientów, których dane mogą zostać upublicznione. Jeśli w wyniku poważnego ataku wyciekły dane karty kredytowej czy dowodu, należy jak najszybciej zastrzec dokumenty i sprawdzać swoją aktywność kredytową w systemie informacji kredytowej BIK.

Trzeba też pamiętać, że istnieje ryzyko ataków phishingowych na klientów, których dane wyciekły: przestępcy mają ich numery telefonu i adresy e-mailowe. Dlatego kluczowa jest ostrożność i powstrzymanie się od klikania linków czy załączników w wiadomościach. Status przesyłki lepiej sprawdzić samodzielnie, wchodząc na stronę sklepu czy firmy kurierskiej. Warto też dbać o bezpieczeństwo kont w innych serwisach – włączyć uwierzytelnianie dwuskładnikowe, nigdy nie używać tego samego hasła w kilku miejscach, regularnie je zmieniać i pamiętać, że powinno być silne. Aby sprawdzić, czy padło się ofiarą cyberprzestępców, na stronie haveibeenpwned.com można zweryfikować obecność swojego adresu e-mail w bazie wykradzionych danych w wyniku dużych ataków. Warto rozważyć też korzystanie z kart prepaid lub wirtualnych, przeznaczonych tylko do zakupów w Sieci.

Raport „State of ransomware in Retail 2021" dostępny jest na stronie: https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-retail-2021-wp.pdf

Zapewnij swoim pracownikom bezpieczną pracę - niezależnie od miejsca

Dzięki Kaspersky ASAP - platformie edukacyjnej online - możesz zadbać, by Twoi pracownicy byli gotowi na cyberzagrożenia, zarówno gdy pracują w biurze jak i w domu.

Nasza platforma powstała przy udziale czołowych ekspertów ds. cyberbezpieczeństwa, dzięki czemu obejmuje najbardziej aktualne i istotne zagadnienia. Zarządzanie szkoleniami jest zautomatyzowane, a pracownicy biorą udział w praktycznych i angażujących lekcjach, które budują ich świadomość i umiejętności z zakresu cyberbezpieczeństwa.

Wypróbuj wersję testową już teraz: asap.kaspersky.pl

kaspersky AKTYWUJ PRZYSZŁOŚĆ

Kaspersky Automated Security Awareness Platform

I to by było na tyle…