2021 prognozy cyberbezpieczeństwa

NET COMPLEX
Bezpieczeństwo IT

33 816 04 11 | www.netcomplex.pl | Wita Stwosza 5 | Bielsko-Biała

JAKI BYŁ 2020?

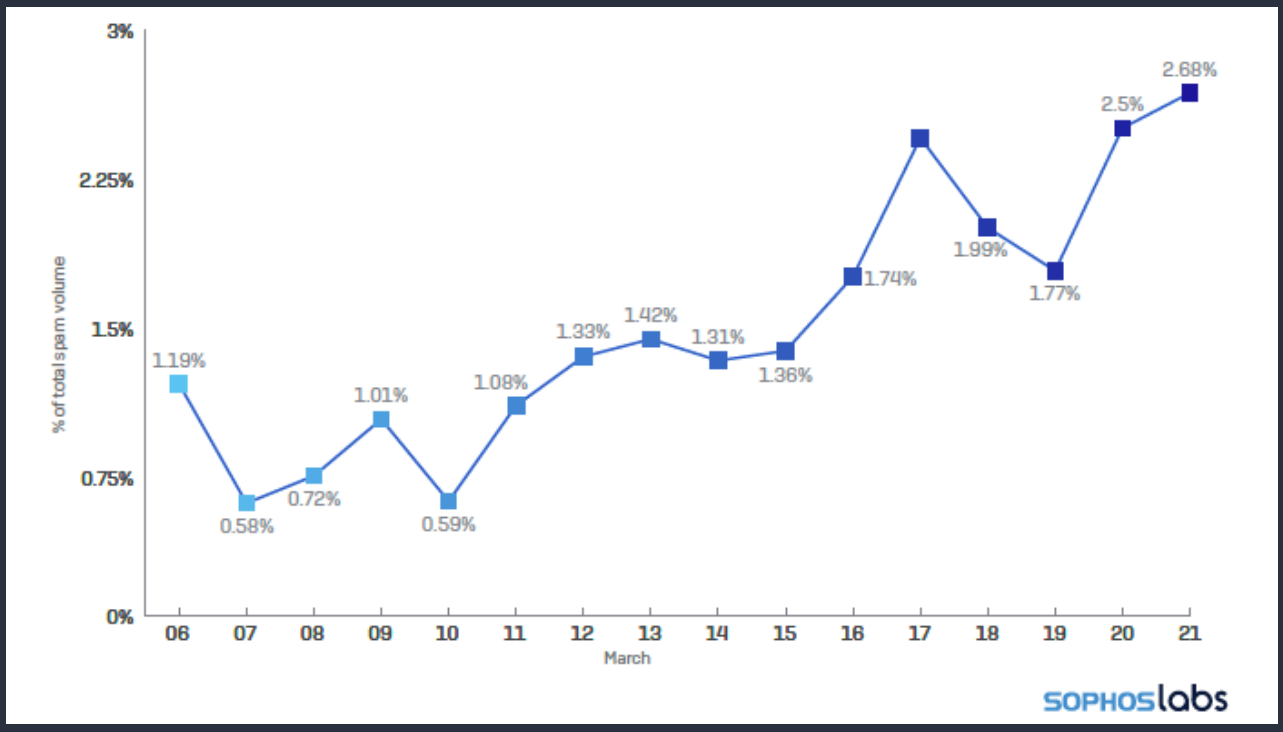
W 2020 roku to pandemia **COVID-19** dała się wszystkim we znaki, również cyberprzestępcom, którzy stworzyli nowe możliwości włamywania się i niszczenia infrastruktury IT. Luki w zabezpieczeniach między siecią domową a biurową odegrały kluczową rolę. Problem doprowadził do kradzieży poufnych informacji, wrażliwych danych, a to spowodowało utratę milionów dolarów poszczególnych organizacji. Wzrosło zapotrzebowanie na zestawy słuchawkowe, mikrofony, platformy do przeprowadzania wideokonferencji, a przede wszystkim -
- **na bezpieczeństwo.**

2020 W LICZBACH:

- 80% firm odnotowało w tym roku wzrost przestępczości;
- koronawirus stał się przyczyną 238% wzrostu ataków na banki;
- ataki phishingowe wzrosły o 600% od końca lutego;
- ataki ransomware wzrosły o 148%;
- w marcu ataki związane z płatnościami online wzrosły o 33%.

NET COMPLEX
Bezpieczeństwo IT

OSZUSTWA E-MAILOWE ZWIĄZANE Z COVID-19



Źródło: Coveware / Sophos labs

ŻĄDANIA OKUPU ZWIĄZANE Z RANSOMWARE WZROSŁY O 21% W OSTATNIM KWARTALE I PRAWIE POTROIŁY SIĘ W CIĄGU OSTATNIEGO ROKU.

Źródło: Coveware / Sophos labs

POPULARNE ATAKI W 2020

1.Software AG Ransomware Attack

Software AG został zaatakowany ransomwarem w październiku 2020r. ZDNet poinformował, że niemieckie przedsiębiorstwo technologiczne zostało zaatakowane przez Clop Ransomware i gang cyberprzestępców, żądając okupu w wysokości ponad 20 milionów dolarów. Raporty donoszą, że firma wciąż nie odzyskała pełnej sprawności. Przyznano, że atak naruszył wewnętrzną sieć, jednak usługi klientów, dane w chmurze nie ucierpiały. Okazuje się, że Software AG próbował negocjować z napastnikami jednak bezskutecznie. Zgodnie z wydanym oświadczeniem, firma jest w trakcie przywracania prawidłowego działania swojego systemu i baz danych.

2. Sopra Steria Ransomware Attack

Francuski gigant usług IT Sopra Steria został zaatakowany przez ransomware 20 października. Sopra Banking Software zidentyfikowała wirusa, będącego nową wersją ransomwera Ryuk. Po weryfikacji, nie zidentyfikowano wycieku żadnych danych. Ryuk to jedno z najbardziej pomysłowych programów ransomwara*, które już atakowało inne organizacje np. EWA, Prosegur.

* Pomysłowych, ponieważ w dawnych czasach Ryuk znany był jako postać fikcyjna w popularnym japońskim komiksie i serialu animowanym. Aktualnie uchodzi za najgorszą rodzinę oprogramowania ransomware, jaka kiedykolwiek nękała systemy komputerowe na całym świecie.

POPULARNE ATAKI W 2020

3. Telegram Hijack

We wrześniu 2020r., hakerzy uzyskali dostęp do Telegramu Messengera i e-maili znanych osób związanych z branżą kryptowalut. Cybeprzestępcy wykorzystali SS7 (Signaling System 7), używany do łączenia sieci komputerowych na całym świecie. Według ekspertów, najprawdopodobniej szukali kodów do logowania, uwierzytelniania dwuskładnikowego. Dodatkowo sfałszowali SMSC operatorów sieci komórkowych, by wysłać prośbę o aktualizacje do co najmniej 20 osób. Uważa się, że atak przeprowadzono w celu zdobycia kryptowalut i mimo, że tego rodzaju zachowania są znane, to nikt nie był przygotowany na tego typu żądania. W tej społeczności istnieją lepsze metody uwierzytelniania niż SMS lub 2FA. Specjaliści uważają, że trzeba odejść od protokołów SS7, które nie radzą sobie w rozwiązywaniu współczesnych problemów.

4. Seyfarth Shaw Malware Attack

Wiodąca firma prawnicza z Chicago, Seyfarth Shaw LLP stała się ofiarą złośliwego oprogramowania. Atak uznano później za ransomware. Zdarzenie miało miejsce 10.10.2020 r. i doprowadziło do całkowitego wyłączenia systemu poczty elektronicznej. W oświadczeniu firmy nie stwierdzono by dane klientów przechwycono, mimo to, podjęto odpowiednie środki zapobiegawcze. Poinformowano organy ściągania, FBI rozpoczęło dochodzenie. Poza tym nie ujawniono szczegółowych informacji na temat tego jak doszło do naruszenia i jak ransomware zaatakował firmę.

POPULARNE ATAKI W 2020

5. Carnival Corporation Data Breach

Największe na świecie przedsiębiorstwo, będące armatorem statków wycieczkowych, zgłosiło naruszenie danych w wyniku ataku ransomware w sierpniu 2020 r. Hakerzy wykradli poufne dane klientów, pracowników i członków załogi. Po zajściu powiadomiono służby, zatrudniono radców prawnych i ekspertów ds. cyberbezpieczeństwa. Firma nie zdecydowała się jednak poinformować jaki rodzaj ransomwarea doprowadził do naruszeń.

6. Twitter

Fałszywy tweet o Bitcoinie. Hakerzy zażądali Bitcoinów od swoich obserwujących, obiecując w zamian podwójny zysk. Mimo tego, że wiadomość była aktywna tylko przez chwilę, znalazło się sporo osób, które zostały ofiarą tego ataku. Sprawcy wykorzystali phishing i phone spear by uzyskać dane uwierzytelniające pracowników Twittera. Ci zaś mieli dostęp do wewnętrznych narzędzi. Hakerzy byli ukierunkowani na 130 kont, tweetowali z 45, uzyskali bezpośredni dostęp do 36 skrzynek odbiorczych, a z 7 kont pobrali dane.

Celem byli: Apple, Uber, a także: Bill Gates, Elon Musk, Jeff Bezos, Warren Buffett, Kanye West, Floyd Mayweather, Barack Obama, Joe Biden, Michael Bloomberg.

POPULARNE ATAKI W 2020

7. Marriot

Marriot to jedna z największych sieci hotelowych (7300 hoteli i 134 obiektów w krajach wypoczynkowych). Firma ujawniła, że w 2020 r. zdobyto dostęp do danych osobowych około 5,2 mln gości hotelowych. Uzyskane treści obejmowały nazwiska, adresy, telefony, daty urodzenia, linie lotnicze. Marriot podał, że informacje o gościach zostały przechwycone w połowie stycznia, za pośrednictwem danych do logowania pracowników w jednym z obiektów franczyzowych. Całość zdarzenia miała miejsce w trudnym okresie, ponieważ podobnie jak inne przedsiębiorstwa turystyczne, zaczęto zwalniać pracowników.

8. MGM Resorts

Udostępniono dane osobowe ponad 10,6 miliona gości MGM Resorts na forum hakerskim. Szczegóły dotyczyły imion, nazwisk, adresów, telefonów, e-maili. Podobno wrażliwe treści obejmowały znane osobistości (m.in. piosenkarza Justina Bibera, dyrektora generalnego Twittera Jacka Dorseya). Według MGM Resorts wyciek danych był spowodowany incydentem z 2019 roku.

9. Finastra

Finastra dostarcza rozwiązania dla światowych instytucji finansowych, w tym do 90 największych banków na świecie. Okazuje się, że również oni padli ofiarą ataku typu ransomware.

POPULARNE ATAKI W 2020

10. Zoom

Przez pandemię Covid-19 Zoom stał się jednym z najbardziej rozpoznawalnych platform wideokonferencyjnych niemal z dnia na dzień. W drugim kwartale firma odnotowała wzrost przychodów aż o 355%. Ja można się domyślić, stali się szybkim i łatwym celem. Około 500 000 kont użytkowników wystawiono na Dark Webie. Hakerzy uzyskali dostęp przy użyciu ID i haseł. Same kody Zoom również były łatwe i użytkownicy mogli dołączać do spotkań bez zaproszenia.

11. Magellan Health

Magellan Health padł ofiarą phishingu, który obejmował eksport danych i uruchomienie ransomwara. Atak dotyczył 8 podmiotów i około 365 000 pacjentów, dlatego do tej pory jest największym naruszeniem mającym miejsce w sektorze opieki zdrowotnej w 2020 roku.

12. Greek Banking System

Po zhakowaniu greckiej strony biura podróży, cztery główne banki w Grecji musiały wymienić/ anulować 15 000 kart kredytowych /debetowych. Alpha Bank, Piraeus Bank, Eurobank, National Bank we wspólnym oświadczeniu stwierdzili, że chociaż tylko kliku klientów zostało obciążonych transakcjami, których nie dokonali, zdecydowali się na podjęcie wszystkich możliwych środków ostrożności.
Pojawia się pytanie, czy witryna posiadała standardy bezpieczeństwa PCI DSS?

CO PRZED NAMI?

2021

Każdego roku w grudniu, przyglądamy się trendom w świecie technologii biorąc pod lupę najnowsze strategie cyberprzestępców. **Jak możemy przygotować się na rok 2021 i kolejne lata?**

Można przewidzieć, że w 2021 roku cyberprzestępcy znajdą nowe, innowacyjne sposoby atakowania osób i urządzeń. Co istotne, to pandemia COVID-19 zdecydowanie przyśpieszyła przejście na pracę zdalną, w której pracownicy działali poza biurem i firewallem. Z całą pewnością, cyberprzestępcy nadal będą wykorzystywać luki pomiędzy urządzeniami a siecią.

ZACZNIJ JUŻ TERAZ PRZYGOTOWYWAĆ SIĘ DO OBRONY PRZED ZAGROŻENIAMI!

NET COMPLEX
Bezpieczeństwo IT

#1

SPEAR PHISHING

To wyrafinowana technika ataku, polegająca na wysyłaniu przekonujących wiadomości e-mail, które zawierają dokładne, szczegółowe informacje na temat konkretnej osoby w firmie. Wiadomości, dobranie kandydata, jest poprzedzone przeprowadzeniem pogłębionego wywiadu środowiskowego na temat potencjalnej ofiary. Cyberprzestępcy pozyskują informacje dostępne w Internecie, na forach, portalach społecznościowych, stronach pracodawcy by jak najlepiej poznać osobę, którą chcą zainfekować.

Te nielegalne działania są bardzo trudne do wykrycia.

Hakerzy już zaczęli tworzyć narzędzia, które mogą pomóc zautomatyzować ręczne wyszukiwanie. Łączą narzędzia z programami skanującymi dane w serwisach społecznościowych.

Phisherzy mogą w ten sposób wysyłać bardzo szczegółowe, wiarygodne wiadomości e-mailowe ze spersonalizowaną treścią. Na pewno zautomatyzowane kampanie będą mniej profesjonalne niż te tworzone ręcznie.

Niezależnie od tego, należy spodziewać się znacznego wzrostu liczby ataków spear phishingowych w 2021 roku z powodu automatyzacji. Co więcej, cyberprzestępcy doskonale wiedzą, że lęk i niepewność sprawia, że potencjalne ofiary łatwiej wykorzystać. Społeczeństwo bowiem, nadal boryka się z wpływem COVID-19, z globalnymi konfliktami politycznymi i ogólnym brakiem poczucia bezpieczeństwa finansowego. Spodziewamy się, że właśnie na tym będą żerować przestępcy.

Ataki phishingowe ewoluowały, przeszły długą drogę, od pamiętnych oszustw „Nigerian Price". Hakerzy dysponują teraz wieloma narzędziami, które pomagają tworzyć przekonujące wiadomości e-mail typu spear phishing, przez co ofiara rezygnuje z poświadczeń lub nieświadomie instaluje złośliwe oprogramowanie.
Ostatnio wykorzystuje się hosting w chmurze, aby oprzeć się na (fałszywej) reputacji przedsiębiorstw takich jak Amazon, Microsoft, Google.

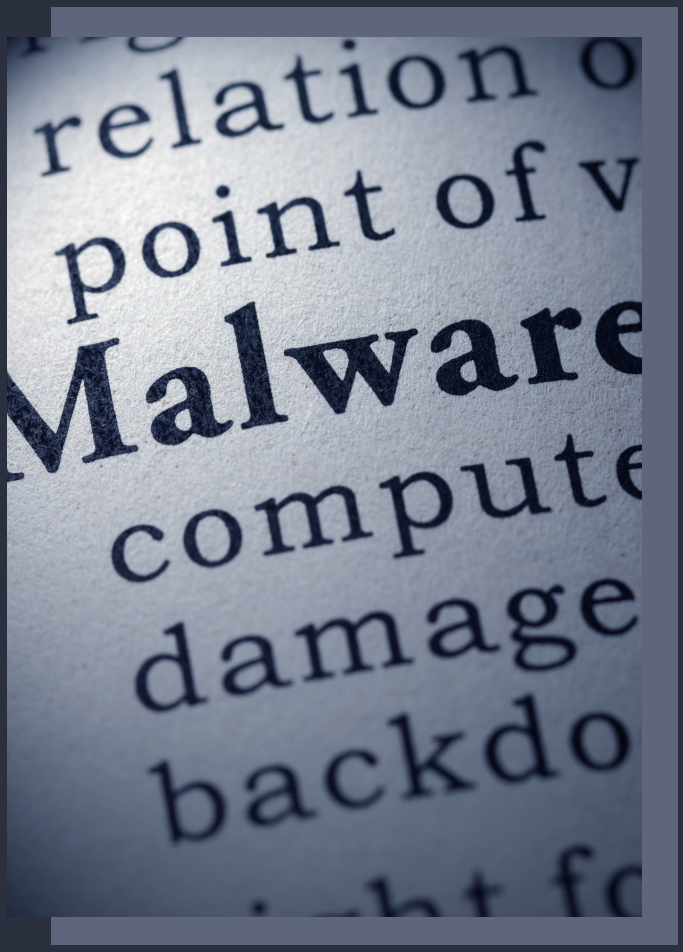
Większość platform hostingowych w chmurze np. Azure, AWS, oferuje przechowywanie danych, użytkownicy mają możliwość przesłania wszystkiego, od kopii zapasowych, baz danych, po pojedyncze pliki. Usługi te są udostępniane w Internecie za pomocą niestandardowych subdomen lub ścieżek URL (np. cloudfronet.net, windows.net, googleapis.com). Cyberprzestępcy często nadużywają tych funkcji do hostowania plików HTML witryn internetowych, które są zaprojektowane tak, aby imitować uwierzytelnianie legalnej strony Microsoft365, Dysku Google.

Ten styl wyłudzania informacji jest skuteczny, ponieważ e-maile odsyłają do sfałszowanych formularzy, przypominających Microsoft Google, Amazon, czy AWS. Dlatego, prawdopodobnie w 2021 roku dostawcy usług hostingowych w chmurze, zaczną zwalczać phishing i inne oszustwa, wdrażając zautomatyzowane narzędzia sprawdzające poprawność plików.

#2

INFEKCJA DOMOWYCH SIECI Z WYKORZYSTANIEM ROBAKÓW

Pandemia zmusiła nas do podjęcia pracy zdalnej, praktycznie z dnia na dzień, dlatego cyberprzestępcy tworzą ataki wymierzone w pracownika **home office.**



Złośliwi przestępcy często umieszczają w szkodliwym oprogramowaniu moduły funkcjonalne - robaki, zaprojektowane tak, aby przenosić się później na inne urządzenia w sieci. **W 2021 roku cyberprzestępcy będą wykorzystywać słabo chronione sieci domowe, by uzyskać dostęp do Endpointów.**

Celowe infekowanie urządzeń w sieci domowej zagraża sieciom korporacyjnym. **W przyszłym roku** spodziewamy się pojawienia złośliwego oprogramowania, które oprócz tego, że będzie rozprzestrzeniało się w sieci, będzie korzystało z VPN.

#3

INTELIGENTNE ŁADOWARKI SAMOCHODOWE W PUŁAPCE HACKÓW

Inteligentne samochody stają się coraz ''mądrzejsze' i powszechniejsze. Bardzo dużo producentów decyduje się na wprowadzanie nowego modelu. Badacze bezpieczeństwa i black hat hackers zwracają na to uwagę. Chociaż w poprzednich latach przyglądaliśmy się wielu interesującym badaniom, od dłuższego czasu odbyło się bez większych incydentów.

W 2021 roku prawdopodobnie hakerzy zdecydują się na wykorzystanie inteligentnych ładowarek.

Podobnie jak w przypadku ładowarek do telefonów i innych urządzeń, inteligentne kable do ładowania samochodów są potencjalnym zagrożeniem. Urządzenia te posiadają komponent danych, który pomaga w zarządzaniu. **Hakerzy i naukowcy, udowodnili już, że w przypadku telefonów, potrafią stworzyć tzw. „ładowarkę pułapkę".** Tak samo, spodziewamy się, że znajdą podobne luki w elementach ładujących do samochodów. Może nawet dojść do takiej sytuacji, w której auto nie będzie mogło się ładować.

#4
PRYWATNOŚĆ URZĄDZEŃ INTELIGENTNYCH

Inteligentne urządzenia są wszechobecne w naszym życiu. Cyfrowe asystentki takie jak Alexa, Google Assistant, Siri obserwują i słuchają wszystkiego co dzieje się naszych domach. Systemy inteligentnych domów zwiększają wartość, wygodę, automatyzując oświetlenie, temperaturę w pomieszczeniach, zamki w drzwiach i nie tylko. Mamy nawet systemy wirtualnej rzeczywistości (VR), które mapują nasze pokoje w 3D za pomocą specjalistycznych kamer, a przy tym wymagają działań w serwisach społecznościowych.

Co więcej, wielu z nas, nosi popularne **smartwatch'e**, które śledzą i wyczuwają parametry zdrowotne (częstotliwość ruchu, bicie serca, EKG, a nawet poziom tlenu we krwi). Dodajmy do tego algorytmy uczenia maszynowego (ML), Firmy technologiczne wykorzystują dane zebrane od użytkowników. **Takie przedsiębiorstwa wiedzą więcej o naszym życiu niż nasi najbliżsi przyjaciele, mogą rozumieć naszą psychologię zachowania lepiej od nas.**

Chociaż wszystkie te technologie są użyteczne, korzystne, społeczeństwo zaczyna zdawać sobie sprawę, że taka inwigilacja nie jest zdrowa. Uczymy się, że algorytmy mapowania, firmy technologiczne używają informacji do kategoryzowania nas, analizują nasze działania i może mieć to konsekwencje dla całego społeczeństwa.

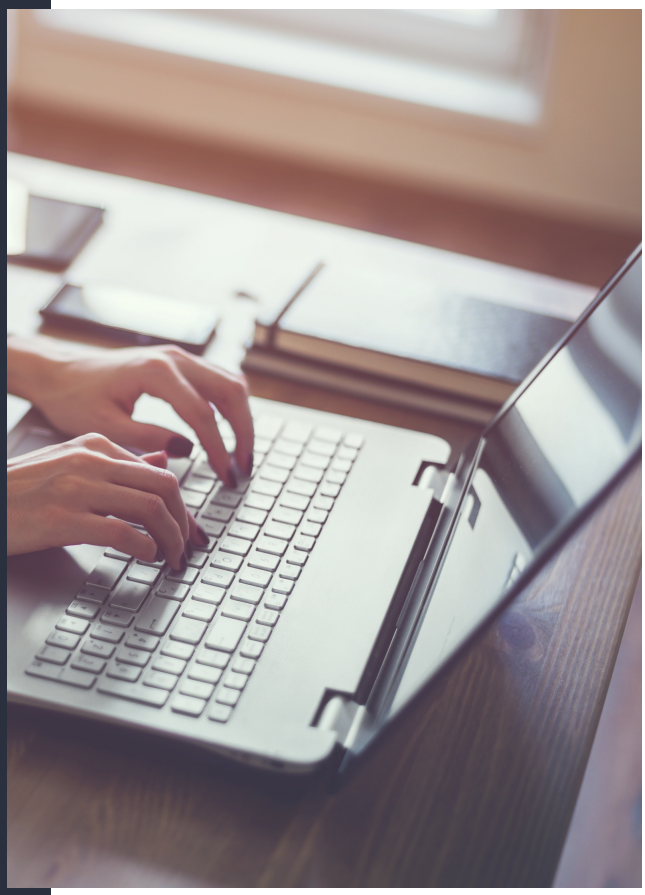
Dlatego w 2021 roku użytkownicy w końcu zbuntują się i sprawią, że sprzedawcy będą poważniej traktować prywatność domowych, konsumenckich urządzeń. Rynek zacznie mocno naciskać na produkty IoT, aby uregulować ochronę prywatności użytkowników.

#5
ATAKI NA VPN I RDP W PRACY ZDALNEJ

Praca zdalna stała się normą dla wielu firm, zmieniła profile oprogramowań i usług, na których opierało się przeciętne przedsiębiorstwo.
Wcześniej wiele osób korzystało z rozwiązań Remote Deskop Protocol (RDP) i VPN Virtual Private Networking (VPN).

Usługi te stały się podstawą umożliwiającą pracownikom zdalny dostęp do danych poza siecią firmową.

Ze względu na to, w 2021 roku cyberprzestępcy zwiększą liczbę ataków na RDP, VPN.



RDP jest jedną z najbardziej atakowanych usług w Internecie, powinna być używana z VPN. Jesteśmy przekonani, że ataki związane z dostępem zdalnym do serwerów podwoją się w 2021 roku.

#6

LUKI W ZABEZPIECZENIACH ENDPOINTÓW

Endpointy stały się priorytetem dla atakujących w czasie pandemii. Ze względu na to, że wiele osób pracuje z domu, bez niektórych zabezpieczeń sieciowych dostępnych w siedzibie firmy, hakerzy koncentrują się na lukach w komputerach osobistych, oprogramowaniu, systemach. Jak na ironię wzrost liczby home office zbiegł się z rokiem, w którym Microsoft zakończył rozszerzoną obsługę Windows 7 Server 2008. Cyberprzestępcy mają szansę wyszukać istotne luki w Windows 7. Podczas gdy systemy Windows 10 i Server 2019 są niedostępne od dłuższego czasu, nie można pominąć faktu, że tylko garstka osób dokonuje aktualizacji. **Windows 7 był jedną z najpopularniejszych wersji przed 10.** Wiele osób uważało 8 za problematyczną, dlatego sporo organizacji zdecydowało się zostać przy wersji 7 i Server 2008. Niektórym przedsiębiorstwom będzie ciężko zrezygnować ze starszych opcji, ponieważ ich urządzenia są skonfigurowane pod stary system. W rezultacie część z nich nadal korzysta ze starych systemów operacyjnych. **Hakerzy doskonale o tym wiedzą i szukają okazji, aby to wykorzystać.**

W 2021 roku możemy spodziewać się co najmniej jednej, dużej luki wykorzystywanej w zabezpieczeniach systemu Windows 7.

#7

BRAK MFA POWODEM NARUSZEŃ

Ataki na uwierzytelnienia stały się codziennością. Cyberprzestępcy odnieśli niesamowity sukces, wykorzystując skradzione nazwy użytkowników i hasła.

PAMIĘTAJ!

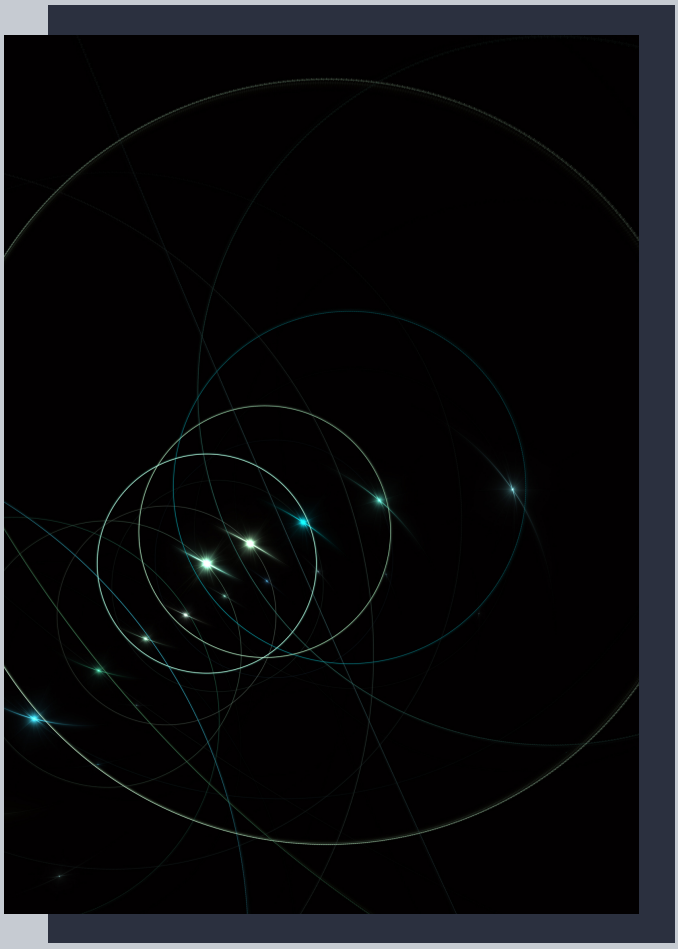
Wybieraj silne, unikane hasła. Wystarczy spojrzeć na Dark Web i fora. Obecnie istnieje miliard szeroko dostępnych użytkowników, haseł pochodzących z włamań. Te bazy danych, w połączeniu z automatyzacją ataków uwierzytelniających, oznaczają, że żadna usługa internetowa nie jest zabezpieczona przed cyberatakami, jeżeli nie korzysta z uwierzytelniania wieloskładnikowego (MFA). **Niestety, w przypadku braku włączonego MFA może dojść do tego, że każda usługa zostanie zaatakowana.**

#8

5G I KOMPUTERY KWANTOWE. NA PEWNO BEZPIECZNE?

W coraz większym stopniu urządzenia brzegowe będą wykorzystywane do ML, szczególnie te zasilane przez 5G. **Cyberprzestępcy będą w stanie przetwarzać ogromne ilości danych, wiedząc jak i kiedy urządzenia są używane.**

Inwestowanie w sztuczną inteligencję nie tylko pozwala na automatyzację zadań, ale także umożliwia tworzenie aplikacji systemowych, które mogą wyszukiwać i wykrywać ataki.



Wiele osób twierdzi, że kwantowość czyni je naturalnie odpornymi na ataki. Komputer wykorzystuje inną metodę reprezentowania i obliczania informacji, dzięki czemu może działać z dużo większą prędkością. Prawdopodobnie, urządzenia te, sprawią, że algorytmy szyfrowania szybko staną się przestarzałe, **a w 2027 roku komputery kwantowe przełamią kryptografię krzywych eliptycznych.**

ZAGROŻENIA 2021

7 NAJWAŻNIEJSZYCH ZAGROŻEŃ WEDŁUG STRAIGHT EDGE TECHNOLOGY*

1

Phishing – uważaj na nietypowe e-maile, mogą zaczynać się od dziwnych sformułowań np. „Szanowny kliencie", zazwyczaj z niepoprawną gramatyką. Zachowaj ostrożność podczas klikania w linki, nie podawaj poufnych informacji, gdy masz wątpliwości - skontaktuj się bezpośrednio ze źródłem, zainstaluj narzędzia anti-phishingowe.

2

SMS-Based Phishing (Smishing) – oparty na wiadomościach SMS (smishing), zawierających odnośnik/link. To typowe wiadomości z „Twojego banku" z prośbą o podanie numeru. **Nie otwieraj linków**, zwróć uwagę na błędy ortograficzne, język, ogólne sformułowania.

3

PDF Scams – podobnie jak w przypadku phishingu, oszustwa PDF mają zamiar skłonić Cię do przeglądnięcia załącznika. Często zawierają informację o aktualizacji polityki lub zachęcają do otwarcia pliku z wyciągiem z konta. **Zwróć uwagę na nietypowe nagłówki, upewnij, że Twój komputer posiada aktualne oprogramowanie antywirusowe.**

4

Malware&Ransomware – Upewnij się, że na bieżąco aktualizujesz przestarzałe oprogramowanie, sterowniki, wtyczki.

5

Database Exposure – Wrażliwe dane stają się celem dla cyberprzestępców. Authentic Jobs, Sonic Jobs przypadkowo ujawnili bazę danych w chmurze, która nie została ustawiona jako prywatna. **Pamiętaj!** Przechowuj sprzęty w bezpiecznych, zamkniętych pomieszczeniach. **Sprawdź swój firewall,** ogranicz dostęp do serwera, zaszyfruj dane i regularnie sporządzaj kopie zapasowe.

6

Credential Stuffing – wypychanie poświadczeń – atak mający na celu kradzież dostępu użytkownika za pomocą danych do logowania (zdarza się często, kiedy wykorzystujesz te same dane logowania w wielu witrynach). Zaimplementuj uwierzytelnianie wieloskładnikowe, używaj różnych haseł. **Nie udostępniaj danych osobom trzecim.** Jeżeli z jakiegoś powodu macie wspólne konto - przekaż informacje ustnie.

7

Accidental Sharing – przypadkowe udostępnienie – np. ''odpowiedz wszystkim'', za pośrednictwem e-maili, niezabezpieczonych formularzy, komunikatorów, mediów społecznościowych. **Ogranicz liczbę pracowników**, którzy mają dostęp do tych samych informacji, zaimplementuj oprogramowanie do monitorowania aktywności, logów.

2021

CO NALEŻY ZROBIĆ?

Należy skupić się nie tylko na **proaktywnej ochronie**, ale także na skutecznej **reakcji na incydenty**. Naruszenia są nieuniknione, potrzebna jest fachowa wiedza. Z drugiej strony nie można oczekiwać, że organizacje będą samodzielne.

Pierwszym krokiem jest śledzenie informacji o zagrożeniach. Kolejnymi: ścisła współpraca z dostawcami, edukacja, partnerstwo z organami ściągania. Zawarcie sojuszu publiczno-prywatnego pozwoli na większe zaangażowanie w działania mające na celu kreowanie bezpiecznej cyberprzestrzeni.

W 2021 r. COVID-19 nadal będzie wpływać na nasze życie, firmy i społeczeństwo, a wpływ ten będzie się zmieniać wraz z upływem roku. Musimy więc być gotowi na serię „kolejnych nietypowych" miesięcy. W związku z przejściem na pracę zdalną, organizacje muszą lepiej zabezpieczyć swoje sieci rozproszone po oddziałach i aplikacje chmurowe, aby chronić swoje zasoby. Oznacza to **egzekwowanie i automatyzację** zapobiegania zagrożeniom we wszystkich punktach sieci - zaczynając od telefonów komórkowych i Endpointów pracowników, kończąc na urządzeniach IoT i chmurze.

Aż 78% organizacji twierdzi, że brakuje im umiejętności cybernetycznych. Edukacja cybernetyczna będzie w 2021 roku wciąż "na topie".

ŹRÓDŁA

1.*Fortinet Cyber Threat Predictions for 2021. An Annual Perspective by FortiGuard Labs.*

2. *WatchGuard Cybersecurity Predictions 2021: https://www.watchguard.com/wgrd-resource-center/cyber-security-predictions-2021.*

3. *Sophos 2021, Threat Report, Navigating cybersecurity in an uncertain world.*

4. *https://securityboulevard.com/2020/10/5-biggest-cyber-attacks-of-2020-so-far/*

5. *https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency*

6. *https://www.straightedgetech.com/5-top-cybersecurity-threats-and-their-solutions-for-2020/*

NET COMPLEX
Bezpieczeństwo IT

33 816 04 11 | www.netcomplex.pl | Wita Stwosza 5 | Bielsko-Biała