Analiza KBN

COVID-19

Seria C Nr 8 (70) / 2020 1 sierpnia 2020 r.

Niniejsza analiza powstała w wyniku realizacji projektu *Bezpieczeństwo narodowe Polski w obliczu pandemii koronawirusa: implikacje wewnętrzne i międzynarodowe* finansowanego ze środków konkursu SocietyNow!#1 w ramach programu Inicjatywa Doskonałości w Uniwersytecie Jagiellońskim.

Dominika Dziwisz

Wpływ COVID-19 na cyberbezpieczeństwo przedsiębiorstw prywatnych – konsekwencje i ryzyko nagłego przejścia na pracę zdalną

Podczas spotkania dyrektorów Microsoftu w 2005 roku Bill Gates powiedział, że w nadchodzących latach wzrośnie konkurencja w walce o zatrudnienie najlepszych, a firmy, które zapewniają dodatkową elastyczność swoim pracownikom, między innymi dzięki pracy zdalnej, będą miały przewagę w tym obszarze. Gates nie mógł wiedzieć, że w 2020 roku praca zdalna nie będzie przywilejem, lecz standardem w warunkach pandemii. W odpowiedzi na atak koronawirusa (COVID-19) w ciągu kilku tygodni pracownicy na całym świecie przeszli na zdalny tryb pracy. Zamiast stopniowego, ostrożnego podejścia do nowych zadań, preferowanego przez większość organizacji, zatrudnieni zostali zmuszeni do nagłej i niespodziewanej pracy z domu. Jednocześnie, poza tą zmianą trybu pracy, nastąpił gwałtowny wzrost prywatnej aktywności w sieci, co przejawia się między innymi częstszymi zakupami internetowymi, korzystaniem z serwisów rozrywkowych online, wyszukiwaniem w Internecie informacji na temat zagrożeń związanych z koronawirusem, wirtualną edukacją, a nawet zdalnymi zajęciami sportowymi.

Praca zdalna w liczbach

Zdecydowanie korzyścią z transferu pracy i części życia prywatnego do przestrzeni wirtualnej jest złagodzenie negatywnych ekonomicznych konsekwencji epidemii dla gospodarki. Jednak błyskawiczne tempo, w jakim odbyła się ta zmiana, rodzi poważne wyzwania bezpieczeństwa. Jednym z nich jest właściwe zabezpieczenie poufności danych, na jakich pracują firmy. W XXI wieku informacja jest bowiem towarem, który można kupić i sprzedać, jak każdy inny produkt, a dane osobowe są niezwykle cennym zasobem innowacyjnych przedsiębiorstw. Dowód ich rosnącej wartości stanowi nie tylko wycena firm będących właścicielami wielkich baz danych, ale także coraz częstsze wycieki danych, włamania hakerów, nielegalny handel danymi i coraz skuteczniejsze metody ich pozyskiwania. Konsekwencją wycieku poufnych danych jest spadek zaufania i wiarygodności firmy.

Oprócz samego zwiększenia skali aktywności w cyberprzestrzeni istotne jest też miejsce, z którego ona pochodzi. W jednej chwili zwykłe mieszkania zyskały nową funkcję biurową, a komputery podłączone do zabezpieczonych sieci biurowych zostały przeniesione w miejsca podatne na ataki hakerskie, gdzie nie przeprowadza się żadnych testów ani nie wymusza standardów bezpieczeństwa. Wreszcie problemem są nie tylko zagrożenia *stricte* techniczne i technologiczne, lecz również nieprzygotowani do pracy zdalnej pracownicy i ich nowe, domowe środowisko pracy. Teraz każdy pracownik jest jednocześnie swoim własnym administratorem IT, inspektorem ochrony danych i specjalistą z zakresu cyberbezpieczeństwa.

Jak wskazują wyniki badań przeprowadzonych w marcu 2020 roku na grupie 2500 respondentów przez firmę rekrutacyjną Devire, do momentu wybuchu pandemii blisko połowa przedsiębiorstw działających w Polsce pracowała zdalnie, ale tylko w pewnym zakresie. Obecnie aż 67% firm, które dotąd nie oferowały możliwości pracy zdalnej, zdecydowało się na taką formę pracy po wybuchu pandemii COVID-19. Jednocześnie 35% polskich firm natrafiło na bariery, które uniemożliwiły wprowadzenie pracy zdalnej, a 13% w ogóle nie miało takiej możliwości. Branże, które z największym udziałem wdrożyły pracę zdalną po wybuchu pandemii, to: nieruchomości (92%), IT (86%), usługi dla biznesu (84%) oraz outsourcing biznesowy i centra usług wspólnych (SSC/BPO, 80%). W dużo mniejszym stopniu praca zdalna znalazła zastosowanie w handlu (35%), administracji publicznej, transporcie, spedycji i logistyce (33%), motoryzacji i lotnictwie (30%). Ma to związek z takimi przeszkodami jak charakter wykonywanych obowiązków (83%), ale także z brakiem sprzętu elektronicznego, w tym przede wszystkim laptopów dostępnych dla wszystkich pracowników (30%). Często wskazywanymi barierami są również brak wiary, że praca zdalna może

funkcjonować sprawnie, brak dostępu do bezpiecznego łącza VPN dla osób pracujących z domu oraz brak regulaminu świadczenia pracy w formie pracy zdalnej.

Mimo takich problemów pandemia COVID-19 bez wątpienia jest katalizatorem transformacji cyfrowej. Jak wykazały badania przeprowadzone przez globalnego doradcę nieruchomościowego Colliers International, wiele przedsiębiorstw planuje dalsze zwiększanie udziału pracy zdalnej w przyszłości. Sami pracownicy nastawieni są pozytywnie do modelu hybrydowego. Wyniki przeprowadzonej w ponad 25 krajach ankiety pośród pracowników biurowych pokazują, że 82% z nich chciałoby pracować zdalnie jeden dzień w tygodniu lub dłużej po zakończeniu kryzysu COVID-19, a 71% osób, które nigdy nie pracowały w domu przed COVID-19, chciałoby w przyszłości pracować zdalnie co najmniej jeden dzień w tygodniu. Ponad połowa ankietowanych uważa, że ich wydajność nie zmieniła się w wyniku pracy w domu, a 24% twierdzi nawet, że wydajność ich pracy wzrosła. Mniej więcej tyle samo osób (23%) uznało natomiast, że ich wydajność spadła. Analiza wydajności pracy w powiązaniu z sektorami wykazała wzrost w branży usług finansowych, usług profesjonalnych i technologii, a spadek w sektorze prawnym oraz edukacji i badań. To pokazuje, że w przypadku niektórych gałęzi biznesu praca zdalna na dłuższą metę się nie sprawdzi, ale wiele firm może z dużym powodzeniem pracować zdalnie.

Epidemia cyberzagrożeń

Podczas gdy wszyscy staramy się przyzwyczaić do „nowej normalności" pandemii COVID-19 w życiu zawodowym i prywatnym, cyberprzestępcy postrzegają kryzys wywołany wirusem jako szansę. Jak podaje kanadyjska firma doradcza SecDev Group, tylko w marcu 2020 roku we Włoszech i USA – krajach szczególnie mocno dotkniętych przez pandemię koronawirusa – natężenie cyberzagrożeń wzrosło o 25–30%. W tym samym okresie dynamika zachorowań na COVID-19 w tych krajach sięgnęła 15–20%, co wskazuje na związek między wzrostem liczby zachorowań a rosnącą liczbą cyberataków.

Metody działań hakerskich w czasie pandemii stają się coraz bardziej wyrafinowane, a masowe przejście pracowników na tryb pracy zdalnej tworzy nowe wektory ataku, jak choćby związane z wykorzystaniem treści dotyczących samej pandemii. W rzeczywistości nie mamy do czynienia z zupełnie nowymi technikami ataku, lecz tymi samymi, na które zawsze byliśmy podatni. Natomiast panika i rozproszenie uwagi na wiele innych prac wykonywanych w domu w czasie pracy zdalnej, jak choćby pomoc w zdalnym nauczaniu dzieci czy codzienne obowiązki domowe, czynią nas bardziej wrażliwymi na stare metody. W obecnej sytuacji dotychczasowe regulaminy działania traktowane są mniej restrykcyjnie i wielokrotnie podejmujemy nieprzemyślane, złe decyzje.

Możliwe, że największym niebezpieczeństwem pracy zdalnej jest samo korzystanie przez pracowników z niezabezpieczonych sieci domowych z wieloma punktami dostępu. Jak podaje ZDNet.com, korzystanie z technologii zdalnego dostępu, takich jak RDP (*Remote Desktop Protocol*) i VPN (*Virtual Private Network*), od początku epidemii koronawirusa wzrosło odpowiednio o 41% i 33%. Jest to związane z wprowadzonymi wymogami bezpieczeństwa pracy w domu i połączenia z wewnętrznymi intranetami za pośrednictwem technologii zdalnego dostępu, takich jak dwie wymienione powyżej. Są to podstawowe narzędzia zapobiegające cyberatakom, jednak pracownicy dla wygody omijają te zalecenia, dodatkowo często pracując na słabo zabezpieczonych bezprzewodowych sieciach prywatnych. Jak podają eksperci portalu Niebezpiecznik.pl, atakujący wielokrotnie korzystają z „otwartej furtki" do sieci domowej. Nierzadko pracownicy korzystają z WEP-a (*Wired Equivalent Privacy*) albo WPA (*Wireless Protected Access*), czyli przestarzałych i niebezpiecznych standardów szyfrowania w sieciach bezprzewodowych z najprostszym hasłem dostępu, domyślnym lub składającym się z daty urodzenia, imienia dziecka czy domowego pupila. Łamiąc hasło, hakerzy uzyskują dostęp do sieci i możliwość przeprowadzenia ataków, na przykład poprzez przechwycenie całej komunikacji, a nawet jej podmianę. Korzystanie z wirtualnej sieci prywatnej (VPN) może zapobiec niektórym atakom, bo uniemożliwia połączenie z serwerem, który przedstawia nieprawidłowy certyfikat. Niemniej jednak nadal narażone na atak są komputery przenośne poszczególnych pracowników. A przestępca, któremu uda się obejść zaporę sieciową na takim komputerze oraz ewentualny program antywirusowy, może uzyskać dostęp również do certyfikatów VPN. Dodatkowym niebezpieczeństwem jest to, że wielu pracowników przetwarza na komputerach osobistych informacje związane z firmą. Niewiele firm z odpowiednim wyprzedzeniem wdrożyło oprogramowanie umożliwiające oznaczanie plików odpowiednim „znakiem wodnym" (ang. *watermarking*) oraz monitorowanie samego sposobu ich przetwarzania i dalszego rozpowszechniania. Oznacza to, że nawet jeśli firma ma przeszkolonych w zakresie cyberbezpieczeństwa pracowników, to bezpieczeństwo danych może zostać narażone na ryzyko przez któregoś z domowników współużytkujących dany komputer. Jeśli dodatkowo uwzględnimy to, że do Internetu podłączonych jest coraz więcej urządzeń – poczynając od telewizorów, a kończąc na ekspresach do kawy, które rzadko kiedy otrzymują aktualizacje bezpieczeństwa i łatwo mogą stać się przyczółkiem przestępcy do dalszego ataku – musimy dojść do wniosku, że typowe środowisko domowe pozostaje szczególnie podatne na ataki.

Mimo to od zarania ludzkości najsłabszym ogniwem wszelkich zabezpieczeń zwykle są ludzie. Zamieszanie związane z pandemią koronawirusa i wymuszonymi nią zmianami w schematach działania przedsiębiorstw jest świetnym punktem wyjścia dla ataków socjotechnicznych. Stąd wynika wzrost częstotliwości ataków phishingowych poprzez wiadomości

e-mail. Często takie informacje pochodzą rzekomo od krajowych lub globalnych organów zdrowia publicznego, które żądają podania danych osobowych w celu uwierzytelnienia bądź otwarcia załącznika zawierającego złośliwe oprogramowanie. Jak podaje Interpol, oszuści często podszywają się pod legalne firmy, na przykład używają podobnych nazw, stron internetowych i adresów e-mail, próbując oszukać nieświadomych zagrożeń użytkowników sieci. Innymi słowy, przestępcy wykorzystują ludzką ciekawość i strach przez zakażeniem. Potwierdzają to opublikowane w kwietniu statystyki Google'a wskazujące, że ich systemy wykrywają dziennie 18 milionów złośliwych i phishingowych wiadomości Gmail związanych z COVID-19, a także ponad 240 milionów codziennych wiadomości spam związanych z COVID. Dlatego tak ważne jest edukowanie użytkowników oraz przeprowadzanie testów socjotechnicznych. Niestety, jak pokazuje raport *It is Security Report, Sir* sporządzony przez firmę Netology na podstawie odpowiedzi 2000 ekspertów bezpieczeństwa z największych firm w Polsce, aż 64% respondentów przyznało, że w ich firmach takie testy nie są przeprowadzane.

Podobnym zagrożeniem dla bezpieczeństwa firmy są także złośliwe aplikacje i fałszywe witryny internetowe wyłudzające dane. Na przykład cyberprzestępcy tworzą fałszywe interaktywne mapy pokazujące rozprzestrzenianie się wirusa i przez nie wykradają dane użytkowników, takie jak hasła. Hakerzy rozpowszechniają złośliwe strony „udające" wiarygodne mapy COVID-19 poprzez media społecznościowe albo wiadomości e-mail. Po otwarciu witryny użytkownik zostaje przekierowany do aplikacji infekującej złośliwym oprogramowaniem, które kradnie informacje poufne. W okresie od stycznia do marca 2020 roku eksperci Check Point zarejestrowali na całym świecie ponad 4000 domen związanych z koronawirusem, spośród których 3% okazało się złośliwych, a 5% zostało oznaczonych jako podejrzane. Jak wykazano, domeny związane z koronawirusem są o 50% bardziej podatne na złośliwe oprogramowanie niż inne domeny zarejestrowane w tym samym okresie.

W czasie pandemii dostrzegalny jest również wzrost liczby złośliwych ataków zawierających oprogramowanie *ransomware*, blokujące dostęp do systemu komputerowego lub uniemożliwiające odczyt zapisanych w nim danych. Jak dowiedziono w najnowszych badaniach Microsoftu, najbardziej dotknięte atakami typu *ransomware* są przedsiębiorstwa sektora medycznego oraz przedsiębiorstwa infrastruktury krytycznej. W ten sposób hakerzy aktywnie pogłębiają kryzys, bo zmuszają najbardziej krytyczne w dobie pandemii przedsiębiorstwa do płacenia okupu w sytuacji, kiedy nie można sobie pozwolić na przestoje. Prawdopodobnie te sieci były obserwowane na długo przed wybuchem pandemii, a hakerzy czekali na odpowiedni moment, aby faktycznie zainfekować system oprogramowaniem *ransomware*.

Rekomendacje

Badania przeprowadzone jeszcze przed pandemią koronawirusa pokazały, że 38% ekspertów bezpieczeństwa z największych firm w Polsce zajmuje się tematem bezpieczeństwa danych dopiero po wykrytych incydentach. Ten wynik jest tym bardziej zaskakujący, gdy weźmiemy pod uwagę, że grupa respondentów pochodzi z organizacji z sektora prywatnego (*enterprise*), gdzie świadomość w obszarze bezpieczeństwa informacji jest bardzo wysoka. Według przeprowadzonego w 2019 roku badania firmy doradczej KPMG cyberprzestępczość dotknęła większość badanych firm w Polsce (68%). Jednak pomimo dużego ryzyka cyberataków zaledwie 57% z nich opracowało procedury reagowania bądź plany zarządzania kryzysowego na wypadek wystąpienia cyberataku. Oznacza to, że mimo świadomości cyberzagrożeń bezpieczeństwo sieci nie jest traktowane priorytetowo i, owszem, bywa monitorowane, ale nie w regularny sposób.

Nieprzygotowanie i brak strategii cyberbezpieczeństwa zbiera żniwo podczas kryzysu wywołanego pandemią koronawirusa. Jest to bolesna nauczka, która wymusi na firmach stosowanie przynajmniej podstawowych standardów bezpieczeństwa. Takie rekomendacje są oficjalnie publikowane na stronach internetowych różnych organizacji, na przykład ENISA (agencja Unii Europejskiej do spraw cyberbezpieczeństwa), oraz firm doradzających w tym zakresie. Zazwyczaj zwracają uwagę na poniższe aspekty:

– edukacja i budowanie wśród pracowników świadomości cyberzagrożeń, stosowanie podstawowych zasad „cyberhigieny", jak między innymi zalecanie stosowania osłon na kamery komputerowe czy niedopuszczanie domowników do komputera, na którym wykonujemy pracę;

– wykorzystanie najbardziej bezpiecznych kanałów wideokonferencji i zapewnienie, że spotkania są zabezpieczone na przykład poprzez konieczność podania hasła do wejścia lub kontrolowanie dostępu gości z poczekalni;

– wymuszenie stosowania połączenia przez VPN i upewnienie się, że sieć jest w stanie utrzymać dużą liczbę jednoczesnych połączeń, a w przypadku braku VPN wzmocnienie bezpieczeństwa domowej sieci wi-fi na przykład poprzez tworzenie silnych haseł, zmianę identyfikatora SSID (nazwy domowej sieci bezprzewodowej), włączenie szyfrowania sieciowego, ograniczenie dostępu do określonych adresów MAC;

– zabezpieczenie dostępu do aplikacji firmowych poprzez mechanizmy uwierzytelniania wieloskładnikowego;

– wdrożenie systemów monitorowania zachowań użytkowników na serwerach i komputerach firmowych, tak by móc wykryć niedozwolone zachowania i zidentyfikować dane, jakie mogły wyciec;

– zapewnienie pracownikom komputerów, które będą im służyć wyłącznie do pracy, z regularnie aktualizowanym oprogramowaniem zabezpieczającym;

– zapewnienie pracownikom wsparcia informatycznego w przypadku problemów technicznych podczas pracy zdalnej oraz sporządzenie instrukcji postępowania na wypadek incydentu bezpieczeństwa;

– tworzenie kopii zapasowych (*backupu*) w chmurze, co rozwiązuje problem przechwycenia i zablokowania ważnych danych, bo wszystkie ważne pliki można odzyskać w jednym momencie.

Większość z powyższych zaleceń jest prosta we wdrożeniu i nie wymaga znacznych inwestycji w kosztowny sprzęt lub oprogramowanie. Natomiast nieprzypadkowo edukacja i budowanie świadomości cyberzagrożeń wśród pracowników stanowi pierwszy punkt na tej liście. To niezbędny składnik każdej strategii cyberbezpieczeństwa. Za zupełnie naturalne uznajemy edukowanie na temat zagrożeń w świecie fizycznym („nie dotykaj urządzeń elektrycznych”, „nie otwieraj drzwi nieznajomym”). Musimy zatem zaakceptować konieczność wpajania podobnych zasad w tym stosunkowo nowym wymiarze ludzkiej obecności, którego znaczenie w ostatnich miesiącach wzrosło jeszcze bardziej.