Coraz więcej firm zwraca uwagę na cyberbezpieczeństwo

Wiele jest jeszcze jednak do poprawy

– Od początku pandemii można było zauważyć wzmożoną aktywność grup hakerskich, ponieważ niecodzienne sytuacje są najlepszym momentem na próby wyłudzenia danych – wyjaśnia Krystian Paszek, ekspert ds. cyberbezpieczeństwa i audytów w firmie DAGMA Bezpieczeństwo IT.

• **Przez ostatnie dwa lata mieliśmy do czynienia z ogromnym rozwojem cyfryzacji i digitalizacji**
FOT. 123RF

ROZMOWA Z
KRYSTIANEM PASZKIEM
z firmy DAGMA Bezpieczeństwo IT

TOMASZ CZOIK: Jak wydarzenia z ostatnich dwóch lat wpłynęły na poziom bezpieczeństwa w sieci?
KRYSTIAN PASZEK: W tym okresie bez wątpienia mieliśmy do czynienia z ogromnym rozwojem cyfryzacji i digitalizacji. Co do samego podejścia do cyberbezpieczeństwa – koniecznie trzeba wspomnieć o dwóch przełomowych momentach. Pierwszym z nich była pandemia koronawirusa, która doprowadziła do przejścia na pracę zdalną tam, gdzie było to możliwe. Wiązało się to z ogromnym wyzwaniem informatycznym, zarówno w kontekście dostępnego sprzętu, jak również w sposobie zabezpieczenia infrastruktury informatycznej.

Administratorzy nie odpowiadali już tylko za sieć, którą zarządzali, ale również za połączenie pracownika korzystającego z własnego domowego dostępu do internetu. Używanie przez pracowników własnej sieci budziło wiele pytań odnośnie do zabezpieczenia infrastruktury informatycznej, monitorowania ruchu sieciowego oraz zachowania samych pracowników. W wielu przypadkach procedury bezpieczeństwa IT nie były dostosowane do pracy zdalnej.

Od początku pandemii można było zauważyć wzmożoną aktywność grup hakerskich, ponieważ niecodzienna sytuacja jest najlepszym momentem na próby wyłudzenia danych poprzez m.in ataki phishingowe (mailowe), które mają nakłonić użytkownika np. na kliknięcie w podany link lub pobranie zainfekowanego załącznika. Atakujący nie tylko skupiali się na próbie pozyskania danych, ale również szukali sposobów przełamania zabezpieczeń infrastruktury informatycznej, bo dynamiczne zmiany mogły pozostawić „furtkę" dla atakującego.

Po kilku, kilkunastu miesiącach większości firm udało się chyba jednak oswoić z tą sytuacją.
– Zgadza się. W momencie, gdy wydawało się już, że przystosowaliśmy się do nowych realiów cyberbezpieczeństwa, nastąpił jednak drugi przełomowy moment, czyli rozpoczęcie wojny w Ukrainie. Z punktu widzenia bezpieczeństwa IT jest on istotny, ponieważ militarny atak został poprzedzony atakami cybernetycznymi skierowanymi na infrastrukturę kluczową Ukrainy. Pokazało to tylko, jak ważną rolę odgrywa w dzisiejszych czasach cyberbezpieczeństwo.

Sytuacja w Ukrainie spowodowała również dużą falę cyberataków składających się z ataków phishingowych, podszywających się pod pomoc naszym wschodnim sąsiadom. Ich celem było pozyskanie cennych danych. Jednym z elementów wojny było i jest również szerzenie dezinformacji. Należy zwracać szczególną uwagę na źródła pochodzenia tych „newsów" i porównywać je ze sprawdzonymi źródłami, nie rozpowszechniając ich w sieci bez weryfikacji.

Należy też pamiętać, że w związku z wojną i kryzysem migracyjnym stopień alarmowy CRP został podniesiony do wysokiego, trzeciego poziomu Charlie-CRP. Jest wprowadzany w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym w cyberprzestrzeni albo uzyskania wiarygodnych informacji o planowanym zdarzeniu. To uświadomiło wielu firmom, że sytuacja jest poważna i z cyberbezpieczeństwem nie ma żartów.

Czy konsekwencją tych wydarzeń była zmiana podejścia do ochrony przed cyberzagrożeniami?
– Oczywiście, że tak. Zmiany w podejściu do tego tematu można zauważyć zarówno w przedsiębiorstwach, jak i u osób prywatnych. Rozumienie cyberbezpieczeństwa w wielu firmach mocno się zmieniło i już teraz można zauważyć, że jest ono traktowane jako coś kluczowego. Zarządy organizacji mają świadomość, że potencjalne ataki mogą doprowadzić do ogromnych strat wizerunkowych i finansowych organizacji. Osoby decyzyjne zrozumiały też, że za cyberbezpieczeństwo odpowiada każdy pracownik firmy, dlatego można dziś zauważyć zwiększone zainteresowanie szkoleniami dotyczącymi bezpieczeństwa IT. Zbudowanie świadomości wśród pracowników przyczyniło się do tego, że nie tylko są bardziej uważni na różnego rodzaju cyberataki, które mogłyby ich spotkać w firmie, ale również zwracają większą uwagę na swoją sieć oraz prywatne dane i zabezpieczenia.

Zjawiskiem, które można zauważyć w wielu firmach w ostatnim czasie, jest tworzenie stanowiska odpowiedzialnego za cyberbezpieczeństwo w danej firmie. Należy jednak zwrócić uwagę, że taka osoba nie zawsze jest w stanie zadbać o pełne bezpieczeństwo sama, ponieważ musi nadzorować wiele zagadnień, m.in. związanych z dokumentacją, procedurami, analizą techniczną czy pracą administracyjną systemów.

Znacznie bardziej odpowiedzialnym krokiem, ale też bardziej kosztownym, jest zbudowanie całego zespołu do spraw cyberbezpieczeństwa. Działania takiego zespołu można podzielić na ofensywne, czyli takie, których celem jest weryfikowanie aktualnego stanu zabezpieczeń i szukania luk i słabych stron (m.in. poprzez próby przełamania tych zabezpieczeń), i defensywne, których celem jest monitorowanie ruchu sieciowego, analiza pojawiających się anomalii oraz blokowanie prób przełamania zabezpieczeń.

Tak jak wspomniałem wcześniej, nie każda firma może pozwolić sobie na takie rozwiązania ze względu na koszty, jakie ze sobą niesie. Wtedy z pomocą mogą przyjść firmy, które świadczą usługi cyberbezpieczeństwa i są w stanie zapewnić powyższe działania na zasadzie outsourcingu. Wiele firm decyduje się dziś na weryfikację aktualnego stanu zabezpieczeń, korzystając z usług firm wykonujących audyty cyberbezpieczeństwa. W ten sposób poznają słabe punkty swojej organizacji, a następnie wdrażają odpowiednie środki mające podnieść poziom zabezpieczeń.

A jak powinniśmy zabezpieczać swoje komputery w dzisiejszych czasach? Oprogramowanie antywirusowe i mocne hasło to absolutne minimum?
– Każdą rozmowę o tego typu zabezpieczeniach zawsze zaczynam od zagadnienia nazywanego przeze mnie „suwakiem" poziomu cyberbezpieczeństwa. To bardzo istotne, bo musimy określić, jaki poziom zabezpieczeń będzie dla nas akceptowalny. Inne narzędzia stosuje prze-

Audyty bezpieczeństwa IT trendem 2022 roku

• Wzrost liczby przeprowadzanych audytów cyberbezpieczeństwa można zauważyć zarówno w jednostkach publicznych, jak również w sektorze prywatnym. Wpływa na to m.in. dynamicznie rosnąca liczba przetwarzanych danych, wyrafinowane działania internetowych przestępców oraz sytuacja geopolityczna. Testy penetracyjne polegające na kontrolowanej próbie „włamywania" się do systemów organizacji przeprowadza się najczęściej z testami socjotechnicznymi pracowników. Poszukiwanie podatności nie polega tylko na sprawdzaniu luk w oprogramowaniu i sieci, ale również m.in. na próbie przechwycenia i przełamania haseł użytkowników, które w realnym ataku mogłyby posłużyć do dalszych działań. Słabe hasła mają wpływ nie tylko na bezpieczeństwo firmy, ale i pracowników, którzy podobne hasła wykorzystują w celach prywatnych.

• Z kolei celem przeprowadzenia testów socjotechnicznych jest weryfikacja wiedzy i sposobu zachowania pracowników na potencjalną próbę ataku. Wykonywanie takich testów przez pracodawcę może przynieść korzyści nie tylko organizacji, ale również pracownikom, którzy dowiedzą się, na co zwracać uwagę podczas korzystania z internetu czy sprzętu komputerowego.

• Bardzo ważne są testy phishingowe, które polegają na wysłaniu spreparowanej wiadomości do grupy adresatów, a następnie na przeprowadzeniu analizy, czy ktoś z pracowników ją otwarł, wszedł we wskazany link i pobrał załącznik. Wiadomości są identyczne do tych, które pracownicy mogą otrzymywać na co dzień. Zmieniona jest tylko domena nadawcy, co symuluje realny atak.

• Wyniki audytów dobitnie pokazują, że im bardziej temat wiadomości jest kontrowersyjny lub odnoszący się do aktualnych wydarzeń, tym więcej osób je otwiera, próbując nawet kilka razy kliknąć w umieszczony w niej link. Odpowiednia edukacja pracowników na temat ataków phishingowych podnosi poziom bezpieczeństwa nie tylko organizacji, ale zwiększa również świadomość społeczną. To pomaga uchronić się przed utratą danych lub też środków finansowych. Zmieniające się sposoby ataków cyberprzestępców i nowe podatności powodują, że cykliczne audyty cyberbezpieczeństwa firm i instytucji publicznych zyskują coraz większą popularność.

cież zwykły użytkownik internetu, a inne np. bank.

Praca z suwakiem polega na przygotowaniu dwóch wariantów zabezpieczenia – na poziomie wysokim i niskim. Na pierwszy rzut oka może się wydawać, że najlepiej od razu wybrać opcję z suwakiem przesuniętym do samego szczytu. To jednak wrażenie mylne – optymalne jest rozwiązanie, które pozwoli nam jak najbardziej zabezpieczyć dane, ale w codziennym użytkowaniu będzie przy tym niezauważalne lub nieznacznie tylko uciążliwe.

Tak jak wspomniałem już wcześniej, w przypadku ustalania zabezpieczeń dla firmy warto najpierw wykonać audyt mający na celu ocenę aktualnego stanu oraz zweryfikować prawdopodobieństwo wystąpienia ryzyka, a dopiero później zaplanować odpowiednie działania podnoszące poziom zabezpieczeń.

W przypadku komputerów domowych poziom zabezpieczeń w wielu przypadków jest niższy. Konieczne jest jednak posiadanie odpowiedniego oprogramowania antywirusowego i stosowanie dwuskładnikowego uwierzytelnienia. Warto też odpowiednio skonfigurować swój router i stosować menedżera haseł, który pozwoli na przygotowanie odpowiednio długich i silnych haseł bez konieczności ich zapamiętywania. Należy pamiętać, że im dłuższe hasło, tym skuteczniejsza ochrona, ponieważ do jego złamania potrzebna jest wtedy większa moc obliczeniowa.

Jak uczulać przed cyberzagrożeniami osoby starsze?

– Dla wielu starszych osób tematyka związana z cyberbezpieczeństwem jest trudna do zrozumienia. Ważne jest, aby małymi krokami pokazywać im, że zastosowanie odpowiednich zabezpieczeń pomoże uchronić ich prywatność oraz cenne dane. Dobrą metodą jest uświadamianie, poprzez wskazanie realnych zagrożeń i praca na suwaku cyberbezpieczeństwa, o którym wspomniałem wcześniej. Pokażmy im, na czym może polegać zagrożenie, a następnie wprowadźmy wspólnie z nimi zabezpieczenie.

Gdy wydawało się już, że przystosowaliśmy się do nowych realiów cyberbezpieczeństwa, nastąpił jednak drugi przełomowy moment, czyli rozpoczęcie wojny w Ukrainie. Pokazało to tylko, jak ważną rolę odgrywa w dzisiejszych czasach cyberbezpieczeństwo

Jakie najpoważniejsze błędy w sieci popełniamy?

– Dzisiejsze ataki nie przypominają już tych sprzed kilku lat, kiedy otrzymywaliśmy wiadomość z nieskładną pisownią informującą np. o otrzymaniu spadku, dzisiaj treść takich maili jest niemal identyczna z prawdziwymi wiadomościami zawierającymi treści, które nie wzbudzają u nas podejrzeń, ale wywołują pewne emocje. Dotyczą one np. pomocy Ukraińcom. Z analiz przeprowadzanych przez nasz zespół ekspertów wynika, że im bardziej kontrowersyjna informacja, tym chętniej w nią wchodzimy często nie weryfikując adresata czy też linku.

Świadomość i wiedza użytkowników internetu jest coraz większa, jednak im więcej korzystamy z sieci, tym większe jest prawdopodobieństwo próby ataku na naszą osobę.

Znając złą sławę danego osiedla, nie zapuszczamy się tam w nocy. Czy potrafimy taką ostrożność przenosić już do sieci?

– Pomimo ciągłego podnoszenia wiedzy jeszcze wiele nam brakuje do tego, żeby podchodzić do cyberbezpieczeństwa tak, jak do bezpieczeństwa fizycznego. Bardzo często uważamy, że jeśli przeglądamy informacje w wygodnym fotelu, a nasze ciało nie odczuwa niepokoju, to jesteśmy bezpieczni. Czasem wydaje nam się też, że po jednym szkoleniu lub po obejrzeniu kilku materiałów jesteśmy w stanie odpowiednio zidentyfikować potencjalny atak, co często osłabia naszą czujność, gdyż jesteśmy zbyt pewni swojej wiedzy. Z doświadczenia wiem, że największą ostrożność w korzystaniu z sieci mają osoby, które zajmują się cyberbezpieczeństwem oraz te, które już doświadczyły ataku.

Rozmawiał Tomasz Czoik