Rzeczpospolita Rachunkowość
15.04.20 nr: 88 str. 2 nakład: 55000 egz.

IT

Cyberbezpieczeństwo w pracy zdalnej

Sytuacja, z którą mamy obecnie do czynienia, kreuje zupełnie nowe podejście do sposobu zarządzania organizacją i jej zasobami. Powodzenie tych zmian, a tym samym przetrwanie firmy, jest silnie uzależnione od tego, jak sprawnie poukładamy procesy biznesowe i jak szybko przestawimy pracowników na nowy sposób pracy.

SEBASTIAN GOSCHORSKI

Dynamika zmian i brak możliwości dokładnego zaplanowania procesów powodują, że organizacje są obecnie w większym, niż do tej pory, stopniu narażone na cyber ryzyko. Warto przeanalizować kilka pomysłów na to, jak chronić swoją firmę przed cyfrowymi atakami,

Wymuszenie pracy w domu spowodowało zmianę wielu naszych nawyków i utartych metod działania. Wiele procesów biznesowych nieoczekiwanie „wyszło" poza mury firm, a w domach powstały wirtualne biura, w których służbowe sprawy mieszają się z prywatnymi. Pandemia i konieczność izolacji zmusiły większość osób do szybkiego poznania wielu narzędzi do pracy zdalnej.

Webinary, wideokonferencje, praca na oprogramowaniu firmowym np. księgowym, stanowiły oczywiście wcześniej elementy naszej pracy, ale – bądźmy szczerzy – był to zazwyczaj margines czasu pracy. Obecnie praca zdalna stała się codziennością, głównym kanałem kontaktu ze współpracownikami i często jedynym sposobem zarobkowania.

Praca z domu

Biuro „domowe" ma oczywiście wiele zalet, takich jak dostępność, elastyczność, brak potrzeby dojazdu do firmy, ale niestety również kilka wad. Sytuacja ta przyczyniła się też do wzrostu zagrożeń związanych z cyberprzestrzenią.

W roku 2019 w Polsce dochodziło do 100 tys. ataków hakerskich dziennie, dzisiaj liczba potencjalnych łatwych celów wzrosła wręcz geometrycznie, a świadomość znacznej części społeczeństwa jak przed nimi się zabezpieczyć, nadal jest – niestety – znikoma. Według magazynu CPO (https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019/) ponad 50 proc. ataków dotyczy małego biznesu, a ich koszty według magazynu Forbes to ponad 6 miliardów dolarów rocznie.

Ataki oczywiście nie dotyczą wyłącznie małego biznesu, a ilość wykradzionych danych może przyprawić o zawrót głowy, np. firma, zajmująca się oceną kredytową, Equifax w roku 2017 utraciła dane ponad 145 milionów osób. Ataku ransomware, czyli ataku programem, który szyfruje dane na naszym komputerze i domaga się zapłaty za ich odkodowanie, dokonuje się co 14 sekund – to częściej niż jest zakładane kolejne nowe konto w social mediach.

Cyfrowe nawyki

Jak wygląda nasza cyber rutyna w czasach kryzysu? Czy pandemia wpłynęła na nie zawsze dobre „nawyki cyfrowe"?

Oto kilka zasad, które pomogą zmniejszyć ryzyko utraty cennych danych firmowych w warunkach pracy zdalnej:

- ograniczenie dostępu fizycznego do urządzeń IT (np. ochrona sprzętu i oprogramowania firmowego przed dziećmi);
- dostęp do systemu firmowego powinien być możliwy jedynie przez wirtualną sieć prywatną (VPN), a także za pomocą uwierzytelniania 2-etapowego (np. hasło do aplikacji i kod weryfikacyjny);
- dostawca oprogramowania VPN nie powinien być wybrany przypadkowo, nie zawsze najtańsze lub najbardziej popularne rozwiązanie jest najlepsze;
- przestrzeganie zasad nadawania i zmiany hasła, wystrzeganie się automatycznego zapisywania haseł i loginów;
- zdalny dostęp powinien być możliwy przez ograniczony czas – konfigurowanie zdalnego połączenia na ograniczony czas (minuty/ godziny), stosowanie automatów wylogowania po czasie tzw. bezczynności;
- zdalny dostęp powinien być ograniczony do niezbędnych zasobów dla danego użytkownika, szczególnie w zakresie danych osobowych;
- aktualizacja systemu operacyjnego i wersji oprogramowania – zaleca się aktualizację organizacyjnych systemów operacyjnych i oprogramowania do najnowszych wersji, ponieważ wielokrotnie nowsze wersje są oferowane przedsiębiorstwom ze względu na naruszenia bezpieczeństwa wykryte w starszych wersjach;
- program antywirusowy powinien być zaktualizowany do najnowszej wersji oraz mieć pełen pakiet bezpieczeństwa, tj. możliwość sprawdzania poczty pod kątem niebezpiecznych programów czy zabezpieczenie w postaci prostego firewalla;
- kopia zapasowa – należy wykonać kopię zapasową dla wszystkich odpowiednich urządzeń i informacji; kopia powinna być wykonywana okresowo w celu weryfikacji integralności kopii zapasowej;
- wszelkie incydenty, które wystąpiły na komputerze używanym w domu, muszą być natychmiast zgłaszane do działów IT w firmie i wyjaśniane;
- wszystkie podejrzane maile muszą być sprawdzone, szczególnie mailowe zlecenia przelewów, pochodzące od osoby nieznajomej, która nie ma powodu, aby przysyłać wiadomość lub załącznik; czerwona lampka powinna się nam zapalić, gdy:
  - w pustej wiadomości znajduje się załącznik;
  - wiadomość nie zawiera żadnych osobistych zwrotów;

KONKURS KSIĘGOWI PRZYSZŁOŚCI

Ruszył I etap online!

Stowarzyszenie Księgowych w Polsce wraz z firmą Soneta sp. z o.o. po raz czwarty zapraszają do udziału w konkursie Księgowi Przyszłości. Rejestracja do konkursu na portalu **ksiegowiprzyszlosci.pl** cały czas trwa! Zachęcamy do zebrania trzyosobowej drużyny i udziału w rywalizacji. Konkurs rozgrywany jest w trzech kategoriach: księgowa zawodowa (KZ), płacowo-kadrowa (PiK), księgowa studencka (KS).
Pierwszy etap zmagań konkursowych rozpoczął się 8 kwietnia br.! Ruszył wyścig po cenne nagrody, nie może Cię w nim zabraknąć!
Więcej informacji na **www.ksiegowiprzyszlosci.pl** oraz **www.skwp.pl**

ZDANIEM AUTORA

Sebastian Goschorski

wiceprezes zarządu Stowarzyszenia Księgowych w Polsce Oddział Okręgowy w Szczecinie; Business Development Partner, Head of China Desk, RSM Poland

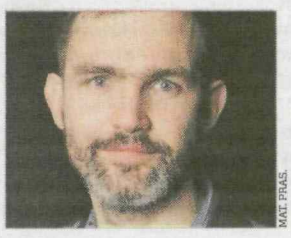

MAT. PRAS.

Reasumując, to co dla nas jest nowe i często pomijane w kwestii cyberbezpieczeństwa, stwarza niesamowite możliwości dla potencjalnych złodziei. Brak odpowiedniego przygotowania, zaplanowania i audytu tego, w jaki sposób umożliwiamy pracę zdalną, może być niezwykle kosztowny. Warto zatem dokładnie sprawdzić system i przetestować go pod kątem możliwości wystąpienia różnych zagrożeń oraz odpowiednio się zabezpieczyć.
W lutym 2019 roku opublikowano pierwszy w Polsce „Raport Cyberbezpieczeństwo: Trendy 2019" (dostępny bezpłatnie: https://www.spidersweb.pl/2019/02/raport-cyberbezpieczenstwo-trendy-2019.html), opracowany przez największe firmy w Polsce zajmujące się bezpieczeństwem. Księgowi często kierują się kosztami. Oto jak do kwestii kosztów odniesiono się w raporcie:
Jednym z największych kosztów, jakie ponoszą niemal wszystkie przedsiębiorstwa dotknięte awarią krytycznych serwerów, jest brak dostępu do świadczonych przez nie usług. Dlatego, kiedy mówimy o zabezpieczeniu infrastruktury, mamy na myśli nie tylko dane, ale także zagwarantowanie bardzo szybkiego, niemal natychmiastowego dostępu wszelkich istotnych usług, jak choćby systemów ERP, czy CRM (...). Szacuje się, że 1 dol. wydany na plan odtwarzania awaryjnego (BCP) przynosi 4 dol. oszczędności w przypadku wystąpienia awarii.
A zatem – księgowa ostrożność opłaca się również w kwestii bezpieczeństwa systemów IT. /®

KOMENTARZ EKSPERTA

Grzegorz Jurczak

ekspert Soneta w zakresie technik produktywności, procesów i analiz biznesowych, kierownik Business Intelligence systemu ERP enova365


MAT. PRAS.

Pandemia wymusiła rewolucyjne zmiany w sposobie wykonywania pracy, jeszcze niedawno niewyobrażalne dla wielu przedsiębiorstw. Wprowadzenie możliwie powszechnej pracy zdalnej, rozproszenie geograficzne, izolacja osób i związane z tym procedury oraz zastosowanie nowych narzędzi powodują zagrożenia, z którymi pracownicy dotąd nie mieli do czynienia.
O ile RODO skłoniło wielu pracodawców do wdrożenia rozwiązań, wymuszających przestrzeganie procedur bezpieczeństwa przetwarzanych danych osobowych, o tyle dopiero teraz przedsiębiorcy zaczynają się zastanawiać nad normami bezpieczeństwa, dotyczącymi narzędzi do pracy zdalnej – związanymi zarówno z komunikacją, jak i prowadzeniem biznesu.
Zatem dostawcę rozwiązań warto zapytać:

- czy systemy przedsiębiorstwa są zainstalowane na certyfikowanych – bezpiecznych serwerach,
- czy komunikacja między użytkownikiem a firmą jest szyfrowana,
- czy na systemach są prowadzone cykliczne audyty bezpieczeństwa a zalecenia wdrażane,
- czy systemy posiadają mechanizmy pozwalające na dostarczenie użytkownikowi niezbędnego minimum danych, pozwalającego na skuteczną i bezpieczną pracę (Workflow czy Business Intelligence)?

Dbałość o bezpieczeństwo jest świadectwem odpowiedzialności managementu za biznes. /®

KOMENTARZ EKSPERTKI

Agnieszka Gajewska

biegły rewident, członek Zarządu Głównego Stowarzyszenia Księgowych w Polsce, wykładowca SKwP


MAT. PRAS.

Na świecie notuje się istotny wzrost ataków na dane, a przestępcy coraz bardziej wykorzystują okazje, jakie stwarza epidemia covid-19. Jedne z najcenniejszych zasobów w firmie to informacje – kontrahenci, pracownicy, umowy, dane finansowe, wysokość uzyskiwanych marż i wiele, wiele innych gromadzonych w formie elektronicznej. Dla konkurencji mogą być bezcenne, a przez obecną sytuację – nieco mniej chronione. Przed pracownikami i pracodawcami stoi zatem ogromne wyzwanie związane z zachowaniem bezpieczeństwa tych danych, zapobieganiem ich wycieku, a w efekcie nawet niekontrolowanego wypływu pieniędzy. Księgowi posiadają dostęp do większości danych wrażliwych dla firmy, warto zatem upewnić się czy posiadamy i czy sprawnie działają procedury awaryjne IT, czy stosujemy zalecenia działów IT dotyczące bezpieczeństwa. Podstawowe pytanie, jakie każdy z nas powinien sobie zadać, to czy znam zasady bezpieczeństwa IT? Może należy ograniczyć dostęp do danych? A jeśli tak, to komu i w jakim zakresie? A może właśnie teraz jest dobry czas, aby zarchiwizować nasze zasoby? /®

KOMENTARZ EKSPERTA

Konrad Antonowicz

szef działu IT Security, Passus SA


MAT. PRAS.

Osoby pracujące z domów, a szczególnie pracownicy z dostępem do kluczowych danych w firmie, mogą stać się celem ukierunkowanych ataków dużych grup cyberprzestępczych. Praca z domu poprzez domowe sieci WiFi stanowi łakomy kąsek dla atakujących.
Sieci takie w większości przypadków są zabezpieczone słabymi hasłami i łatwo dostać się do nich, aby podsłuchiwać komunikację lub/i podmienić ustawienia domowego routera (np. przekierowanie DNS na strony phishing'owe itp). Dlatego, poza zmianami wprowadzanymi w infrastrukturze firmowej, warto również zadbać o swój własny ogródek.
Należy pamiętać o zmianie hasła routera z defoultowego, zaktualizowanie przeważnie dziurawego i nigdy nieaktualizowanego firmware, a co najważniejsze – wymianę hasła dostępowego do sieci. Dobrą praktyką jest wygenerowanie go za pomocą managera haseł, lub podmienianie minimum co dwa tygodnie. Należy pamiętać, że protokoły WPA/WPA2 są bardzo podatne na atakowanie danych uwierzytelniających, a odpowiednie słowniki pozwalają na szybkie złamanie wygenerowanego hasła (sprzęt do takiego ataku można skompletować za kilkanaście złotych).
Dodatkowo bardzo ważne jest stosowanie dwuskładnikowego (2FA) uwierzytelniania do połączeń VPN i logowania do kluczowych aplikacji, ponieważ złe praktyki zapamiętywania haseł na komputerach mogą powodować, iż osoba trzecia, wchodząca w posiadanie naszego komputera, dostanie również pełny dostęp do danych na serwerach firmowych.
Kolejnym ważnym elementem są komunikatory, które znacznie ułatwiają kontakt ze współpracownikami, ale mnogość ich posiadania stanowi zagrożenie, iż przez przypadek możemy wysłać dane nie tam, gdzie chcemy. Dodatkowo niemonitorowane przez pracowników bezpieczeństwa komunikatory mogą być dla nieuczciwych lub nieuważnych pracowników doskonałym kanałem wycieku informacji.
Warto również pamiętać o ujawnianych co chwila podatnościach na różnego rodzaju komunikatorach (np. whatsup), które stanowią idealną furtkę do zainfekowania komputera pracownika i wycieku danych. Dlatego należy dbać o ich aktualizacje i monitorowanie wersji tego typu oprogramowania, a także zachować czujność i zdrowy rozsądek przy korzystaniu z komputera i ułatwień, jakie oferuje. /®

Rzeczpospolita Rachunkowość
15.04.20 nr: 88 str. 2 nakład: 55000 egz.

- wiadomość podpisana jest przez nadawcę, którego dane adresowe ze stopki e-mail nie odpowiadają danym w domenie, z której e-mail został wysłany;
- załącznik ma nazwę o podwójnym rozszerzeniu, np. NAZWA.JPG.vbs;

- przesyłanie załączników w mailach powinno być ograniczone do minimum, należy korzystać z szyfrowanych przesyłów w chmurze, tj. na wydzielone części dysków wspólnych;
- narzędzia do pracy zdalnej, szczególnie do wideokonferencji, powinny mieć funkcje szyfrowania danych – często najbardziej popularne programy pod względem bezpieczeństwa są bardzo słabe zabezpieczone;
- wszelkie dane, które pobieramy z firmy, powinny być przekazywane przy pomocy rozwiązań chmurowych, a nie fizycznego nośnika, np. pendrive'a czy karty pamięci; pracownicy muszą mieć świadomość dbania o bezpieczeństwo informacji, w szczególności o dane wrażliwe;
- posiadanie właściwej polisy od cyber ryzyka, która zapewni pomoc w przypadku utraty ważnych danych osobowych, pokryje koszty reakcji i zarządzania kryzysowego;
- przestrzeganie wszystkich procedur RODO we właściwy sposób, np. w przypadku biur rachunkowych – odpowiedni obieg dokumentów klientów.

Należy pamiętać, że praca z domu poprzez VPN wiąże się zazwyczaj z wolniejszym dostępem do zasobów firmowych zgromadzonych, np. na dyskach wspólnych. Może to dawać dostęp do tych zasobów na dużo gorzej zabezpieczonych komputerach domowych czy na dyskach przenośnych. W tym przypadku, oprócz ryzyka ich utraty, np. w wyniku uszkodzenia dysku, wystawiamy je w znacznie większym stopniu na ryzyko kradzieży. Zabezpieczeniem jest na pewno stworzenie możliwości automatycznej synchronizacji danych na komputerze domowym z dyskiem sieciowym firmy w chmurze obliczeniowej dostarczanej przez sprawdzoną firmę.

UWAGA!

Za nieprzestrzeganie przepisów związanych z RODO grozi odpowiedzialność cywilna, karna i sankcje w postaci administracyjnych kar pieniężnych.

Nowe cyber możliwości

Przedstawione wytyczne nie różnią się, oczywiście, znacząco od typowych zasad zapewniania bezpieczeństwa cyfrowego. Warto jednak pamiętać, że czas pandemii otwiera przed hakerami nowe możliwości, gdyż udostępniając zasoby swojej firmy pracującym zdalnie pracownikom, ułatwiamy też działanie cyberprzestępcom. Z pewnością należy zwrócić pracownikom uwagę, że złe nawyki z pracy stacjonarnej mogą być wielokrotnie bardziej niebezpieczne w warunkach pracy zdalnej.

Warto w tym celu przygotować listę kontrolną – proste pytania, na które może odpowiedzieć pracownik niebędący inżynierem informatykiem. Dla pracowników biura rachunkowego taka lista powinna zawierać, m.in.:

- prośbę o sprawdzenie aktualizacji oprogramowania, zarówno księgowego jak i antywirusowego;
- prośbę o sprawdzenie bezpieczeństwa haseł do systemów, czy są zapamiętane, a nie np. zapisane na karteczce przyczepionej do monitora;
- przypomnienie o konieczności zapisania plików, nad którymi pracujemy w firmowej chmurze, tak żeby były bezpieczne i dostępne w przyszłości;
- przypomnienie o nieotwieraniu podejrzanych maili z nieznanego źródła i każdorazowe sprawdzanie takiej wiadomości programem antywirusowym, a w razie konieczności poinformowanie właściciela biura;
- przypomnienie o niepodawaniu w żadnym wypadku hasła do systemów przez telefon zarówno nieznanym, jak i znanym osobom;
- prośbę o sprawdzenie czy w przypadku zakończenia pracy system został właściwe zamknięty – często brak odpowiedniego wylogowania może zablokować możliwość korzystania z programu kolejnemu użytkownikowi. /®