Praca zdalna. Standardowe podejście do bezpieczeństwa to za mało.

Od kilku miesięcy słyszymy o wzmożonej działalności hakerów wykorzystujących to, że wiele osób przeniosło swoją aktywność zawodową do własnych domów. Słabo zabezpieczony sprzęt, niepotrzebne dostępy do danych firmowych, współdzielenie komputerów z bliskimi czy w końcu zwykła nieostrożność mogą wyrządzić przedsiębiorstwom ogromne szkody. Czy da się im zapobiec? Pomogą technologie, zewnętrzni doradcy oraz szkolenia pracowników.

Jeśli miałbym sformułować jedną z najważniejszych zasad bezpieczeństwa firmy, powiedziałbym, że jest nią edukacja użytkowników, weryfikacja ich działania i bezwzględna egzekucja realizacji procedur.

Łukasz Włodarczyk, Senior Solutions Architect INNERGO Systems

Dzisiejszy biznes opiera się na informacji. I to ona jest najcenniejsza dla cyberprzestępców. Nic zatem dziwnego, że szukają wszelkich dróg, aby zdobyć jak najwięcej danych – handlowych czy finansowych. W czasach pracy zdalnej łatwy dostęp do informacji to także podstawa efektywnego działania przedsiębiorstw.

- *Brak dostępu do danych w dobie COVID-19 w znacznym stopniu utrudnia funkcjonowanie organizacji. Z drugiej stronu utrata danych może wpłynąć na jej renomę, wizerunek czy całkowicie pozbawić możliwości działania – świadczenia usług lub realizacji sprzedaży. Weźmy niedawny dosyć głośny przypadek jednej z firm kosmetycznych, którą utraciła całkowicie płynność produkcyjną, logistyczną oraz sprzedażową, ponieważ do zagadnienia bezpieczeństwa nie podeszła globalnie, całościowo i kompleksowo. Mały błąd może kosztować wiele. Także w kontekście realnych kar finansowych za naruszenia RODO* – mówi Łukasz Włodarczyk, Senior Solution Architect z Innergo Systems.

Firmy muszą tak zorganizować swoją działalność, aby z jednej strony pracownicy mogli bez problemów łączyć się z firmowymi bazami, a z drugiej – hakerzy nie mieli szans wykraść cennych informacji. Jak to zrobić?

Po pierwsze: sprawdź, co masz

Nową organizację pracy firmy należy rozpocząć od inwentaryzacji danych i zasobów. Najważniejsze jest to, aby jednoznacznie określić i sklasyfikować dane, jakimi firma dysponuje, przypisać je do odpowiednich grup i nadać im stopień poufności. Następnie należy ustalić, kto do tak skatalogowanych informacji powinien mieć dostęp oraz sprawdzić, czy w firmie nie ma pracowników, którym niepotrzebnie nadano dostępy do niektórych baz. Jeśli tak jest, trzeba odebrać możliwość wglądu do danych osobom, które w rzeczywistości nie potrzebują tego do pracy. Im mniej źródeł dostępu do wrażliwych informacji, tym mniej potencjalnych miejsc ataków na infrastrukturę firmową.

Po drugie: postaw na technologie

Nie da się jednoznacznie wskazać najlepszego rozwiązania, które pozwoli na sprawną i bezpieczną pracę zdalną. Technik działania, technologii i sposobów jest wiele. Ważne jest to, aby podejść do takiego zadania racjonalnie, mając na uwadze posiadaną infrastrukturę, systemy oraz zasoby. Najczęściej wykorzystywaną technologią jest tunel VPN.
VPN – w powszechnym rozumieniu – to aplikacja na stacji roboczej służąca do bezpiecznego łączenia się do sieci. Rynek pokazuje jednak, że coraz większa rzesza firm wyposaża swoich pracowników w zdalne urządzenia, np. bezprzewodowe punkty dostępowe, pozwalające na dostęp do krytycznych obszarów firmy. Jak zabezpieczyć takie sprzęty?

- *Na pewno warto skonsultować się z integratorem, firmą doradczą lub konsultantem, by zamiast inwestować w nowe kosztowne bramy, firewalle lub koncentratory VPN, móc wykorzystać posiadaną infrastrukturę, kontroler sieci bezprzewodowej lub maszynę wirtualną, kupując np. tylko licencje* – tłumaczy ekspert z Innergo Systems.

Jeśli firma zdecyduje się na VPN-y, musi pamiętać o odpowiednich algorytmach szyfrowania i długości klucza, bo to one mają gigantyczny wpływ na to, jak szybko dane zabezpieczenie może zostać złamane.

- *Prawdą jest, że każde zabezpieczenie w odpowiednich warunkach, da się przejść, złamać lub obejść. Dlatego tak ważną rzeczą – poza odpowiednim przygotowaniem zasobów, sposobów dostępu, mechanizmów zabezpieczeń – jest monitorowanie i reagowanie na zdarzenia. Każdy alarm, znikające pliki, dziwne maile lub nawet telefony z pytaniem, jakiego antywirusa używacie, powinny być impulsem do chociaż podstawowej analizy ewentualnego wpływu na przyszłe działanie i nieustanne edukowanie wszystkich pracowników* – wyjaśnia Łukasz Włodarczyk.

Bliskim ideału rozwiązaniem do pracy zdalnej jest sesja zdalnego pulpitu z firmowego komputera wyposażonego w Endpoint Protection, logowanie domenowe lub podwójne uwierzytelnienie, zastosowanie antywirusa, ochrony DNS i połączenie poprzez VPN zestawiany na dedykowanym urządzeniu.

Po trzecie: pamiętaj o słabościach

Wszystkie te zabezpieczenia będą jednak niewystarczające, jeśli pracownik udostępni swój komputer osobie niepowołanej. Dlatego polityki bezpieczeństwa stosowane w firmach powinny zakazywać pracy na prywatnych urządzeniach.

- *Takie sprzęty mają zazwyczaj wielu użytkowników, a tym samym są wykorzystywane do różnych działań. W swoim dorobku widziałem przypadki wycieku danych spowodowane niefrasobliwością pracowników udostępniających komputer dziecku, by mogło obejrzeć film lub zagrać w grę online. Jeśli dodatkowo taki komputer nie ma podstawowych mechanizmów antywirusowych, korzystanie z portali o miernej reputacji w obszarze malware i innych zagrożeń staje się prostą drogą do utraty firmowych danych* – mówi Łukasz Włodarczyk.

Innym potencjalnym zagrożeniem może być prywatna lub otwarta sieć WLAN. W tym przypadku sprawdzi się poprawne zastosowanie VPN-a na komputerze służbowym. Nawet jeśli użytkownik ustawi słabe hasło, podsłuchanie takiej sesji będzie praktycznie niemożliwe. Dodatkowo aplikacje na firmowym sprzęcie – takie jak popularne na rynku pakiety typu Internet Security z antywirusem i regułami zgodnymi z polityką firmy – wystarczą do wyeliminowania wielu zagrożeń.

Co jeśli firma nie jest w stanie zapewnić służbowych komputerów wszystkim pracownikom zdalnym?

- *W miarę bezpiecznie z dowolnego, prywatnego komputera da się korzystać tylko wtedy, gdy zastosujemy dobrze sprofilowany VPN i zdalny pulpit. W takiej sytuacji dane są przechowywane oraz przetwarzane jedynie w firmie, a użytkownik widzi obraz sesji na serwerze. Oczywiście wciąż zagrożeniem pozostaje wyciek hasła lub nieautoryzowany dostęp do niego. Przechowywanie go w pękach kluczy przeglądarki czy repozytorium w MacOS nie jest dużym problemem, jeśli mamy szyfrowany dysk. Zgoła odmiennie wygląda to w przypadku MS Windows. Jeśli użytkownik sam świadomie nie uruchomi chociaż BitLockera, który dostępny jest w wersjach OS powyżej Home, to przy fizycznym dostępie do laptopa można to hasło odczytać* – przestrzega ekspert z Innergo Systems.

Po czwarte: zadbaj o wiedzę

Powyższe przykłady pokazują, że w całym systemie zabezpieczeń budowanym przez firmę newralgicznym ogniwem jest człowiek, czyli użytkownik, który nieprzemyślanymi zachowaniami może zniweczyć wysiłki działu IT, dostosowującego infrastrukturę do realiów pracy zdalnej.

Dlatego tak istotne jest z jednej strony wprowadzenie odpowiednich polityk bezpieczeństwa, z drugiej zaś – regularne szkolenia dla pracowników, nie tylko wyjaśniające reguły wdrożone w przedsiębiorstwie, ale też przybliżające najnowsze zagrożenia, sposoby działania cyberprzestępców oraz możliwości przeciwdziałania im.

- *Jeśli miałbym sformułować jedną z najważniejszych zasad bezpieczeństwa firmy, powiedziałbym, że jest nią edukacja użytkowników, weryfikacja ich działania i bezwzględna egzekucja realizacji procedur* – podsumowuje Łukasz Włodarczyk z Innergo Systems.

Po piąte: zapytaj ekspertów zewnętrznych

W teorii przygotowanie do pracy zdalnej może wydawać się proste, jak jednak wdrożyć te założenia w praktyce? Warto skorzystać z pomocy ekspertów zewnętrznych, którzy pomogą przeprowadzić niezbędne audyty oraz zaproponują najlepsze rozwiązania.

- *Przede wszystkim należy zacząć od analizy tego, co mamy, zaktualizować w miarę możliwości oprogramowanie wszystkich urządzeń, przeprowadzić audyt konfiguracji nie tylko w zakresie funkcjonalnym, ale także możliwych zabezpieczeń, czyli przeprowadzić tzw. hardening* – tłumaczy Łukasz Włodarczyk.
– Z pomocą doradców zewnętrznych takie działania są po prostu łatwiejsze i efektywniejsze.

Eksperci wybiorą też dla firmy odpowiednie technologie, oparte na różnych platformach bezpieczeństwa i różnej logice zabezpieczeń oraz przynajmniej dwóch repozytoriach. Zrewidują konfigurację VPN, wykorzystywane metody szyfrowania oraz długości kluczy. Dodatkowo zadbają o wydajność technologii czy ograniczenie kosztów.
- Jeśli na przykład firewall zapewniać będzie analizę ruchu, wykrywanie intruzów i dodatkowo przekierowania, to jego wydajność może się okazać niewystarczająca do podłączenia niezbędnej liczby użytkowników, co w najgorszym przypadku skutkuje decyzją o wyłączeniu zabezpieczeń. A to nigdy nie powinno mieć miejsca. W takiej sytuacji lepiej zakupić dodatkowe, słabsze, tańsze urządzenie, które będzie wyręczało Firewalla w zakresie VPN, niż rezygnować z odpowiednich zabezpieczeń w innym obszarze. Wielu klientów nie jest też świadomych tego, że terminowania tuneli VPN można dokonać na niektórych przełącznikach, kontrolerach WLAN, zacznie upraszczając implementację rozwiązania oraz redukując koszty – mówi Łukasz Włodarczyk.

Obecna sytuacja globalna zmusiła firmy do zmiany myślenia o organizacji pracy. Kluczowe stało się zapewnienie, utrzymanie i rozwój infrastruktury IT odpowiedzialnej za bezpieczeństwo firmy. Uzupełnieniem oprogramowania i sprzętu musi być też stałe uświadamianie pracowników. Tylko kompleksowe podejście do bezpieczeństwa pozwoli maksymalnie ograniczyć zagrożenia, jakie czyhają na przedsiębiorstwa w dobie pracy zdalnej.