„Chcieliśmy ewolucję, a dostaliśmy rewolucję”

22 czerwca 2020

Paweł Wałuszko, Business Development Manager, Cybersecurity Expert z TestArmy CyberForces w materiale dla ISBtech w kwestii cyberbezpieczeństwa w pracy zdalnej.

Błąd ludzki oraz celowe działania pracowników to powody ok. 55-59% wszystkich incydentów cybernetycznych. Dlatego dziś, w dobie pracy zdalnej, kiedy nadzór nad kadrami jest zdecydowanie trudniejszy, firmy są jeszcze bardziej niż wcześniej podatne na ataki cyberprzestępców. I dlatego home office to nie ewolucja a rewolucja dla polskiego środowiska biznesowego.

Jeszcze przed wybuchem pandemii, w Polsce chęć wykonywania przynajmniej części pracy w formie zdalnej deklarowało aż 61% pracowników (badania „Confidence Index” przeprowadzone przez Michael Page w IV kwartale 2019 r.), a home office miało ok. 4,8% z nich, co dawało nam wynik stanowczo poniżej średniej Unii Europejskiej.

Przed nami były praktycznie wszystkie kraje Europy Zachodniej. Dla porównania, w tym samym okresie w Stanach Zjednoczonych zdalnie obowiązki służbowe realizowało aż 18% pracowników. Eksperci przewidywali też, że trend ten będzie systematycznie wzrastał.

Sytuacja diametralnie zmieniła się w momencie wybuchu pandemii. Według danych Głównego Urzędu Statystycznego, w marcu br. pracę zdalną wykonywało już 14,2% badanych (przy ogólnej liczbie pracujących). Co więcej, w całym pierwszym kwartale 2020 r. wskaźnik ten wyniósł 11%, podczas gdy w poprzednim oscylował na poziomie około 4,3%.

Biorąc te liczby pod uwagę można dedukować, że większość pracowników zaczęła pracę zdalną właśnie w ostatnich miesiącach. Ponadto okres pandemiczny, zależnie od tego jak

długo będzie się utrzymywał, oraz potencjalna druga fala zachorowań mogą spowodować jeszcze większe zainteresowanie pracą zdalną.

Dlaczego biznesowi trudno zaakceptować home office?

Jedną z podstawowych przyczyn, dla których polskim przedsiębiorcom trudno przestawić się na pracę zdalną jest brak możliwości kontroli i nadzoru pracy pracownika, do których zostali przyzwyczajeni. Aby zyskać wspomnianą kontrolę, wielu z nich regularnie przeprowadza wideokonferencje lub korzysta z komunikatorów.

Tutaj barierą dla przedsiębiorców są jednak kwestie z bezpieczeństwa, ponieważ to, co jest wygodne, niekoniecznie jest bezpieczne. Szczególnie, że nawet gdy istnieją dobre alternatywy przygotowane przez pracodawcę, część pracowników ma tendencję do korzystania z tego, co wydaje im się bardziej wygodne lub znajome.

Drugim aspektem jest sama organizacja pracy. W przeciwieństwie do pracy w biurze, pracownik zdalny musi polegać na samoorganizacji i własnych procedurach zarządzania czasem. Te natomiast nie zawsze są tak wydajne, jak np. przy współpracy z menedżerem lub zespołem. Konsekwencją tego mogą być np. opóźnienia lub zaniżona jakość wykonywanej pracy.

Trzecim, dość często wymienianym problemem związanym z pracą zdalną jest dostęp do danych, a dokładniej bezpieczeństwo informacji znajdujących się poza biurem. Po pierwsze, przedsiębiorstwo musi zadbać o bezpieczny transfer danych, co wiąże się z uzewnętrznieniem części usług dostępnych dotychczas tylko wewnątrz sieci. Oczywiście, część firm korzysta z infrastruktury chmurowej, więc teoretycznie ta sytuacja nie wprowadza wielkich zmian (dane już są przechowywane w centrach danych na terenie całego kraju lub np. Unii Europejskiej).

Inne przedsiębiorstwa wykorzystują technologię VPN, która umożliwia bezpieczne, zdalne łączenie się z siecią wewnętrzną, dzięki czemu dane pozostają na fizycznych serwerach firmy. To, co jednak łączy oba rozwiązania to fakt, że muszą być podłączone do urządzenia, które z natury połowicznie funkcjonuje poza kontrolą działu IT.

Poza tym dochodzi problem fizycznego bezpieczeństwa danych. W przeciwieństwie do komputerów w biurze, do urządzeń w domu pracownika mogą mieć dostęp osoby postronne. Pracodawca nie może mieć pewności co do jakości ich zabezpieczeń antywłamaniowych. Teoretycznie, nawet gdy komputery są szyfrowane, pendrive z danymi może zniknąć.

Jest problem? Są rozwiązania!

W dobie pracy zdalnej z pomocą przychodzą rozwiązania technologiczne. Warto podkreślić, że w przypadku kwestii bezpieczeństwa najlepiej podejmować decyzje świadomie, kompleksowo podchodząc do problemu, zamiast zlecać nadzór nad bezpieczeństwem wyłącznie działom IT.

Rozwiązania informatyczne są kosztowne i spełniają swoje technologiczne funkcje. Natomiast legalność, sposób funkcjonowania i faktyczne wykorzystywanie przez pracowników po ich wdrożeniu to zupełnie inny temat.

Monitorujmy, ale z dystansem

Na polskim rynku istnieje wiele rozwiązań monitorujących, pochodzących od krajowych producentów oprogramowania. Można podzielić je na dwie kategorie: systemy monitorujące sieć i metadane oraz systemy monitorujące wydajność pracownika.

W pierwszej kategorii możemy znaleźć rozwiązania, które m.in. pomagają określić, kto faktycznie używa zasobów firmy i w jakim zakresie. Można z łatwością sprawdzić czy pracownik sprawdza prywatnego maila lub streamuje filmy, choć bez wglądu do przesyłanych danych.

W drugiej kategorii systemów monitorujących są te bardziej inwazyjne, np. zbierające konkretne dane m.in. o tym, jaki program jest najczęściej używany, ile czasu pracownik spędza przed komputerem oraz które zadania zajmują mu najwięcej czasu. Aby uzyskać takie dane, oprogramowanie może wykorzystywać np. kamerę do nagrywania lub oszacowania faktycznego czasu spędzonego przed komputerem.

Niektóre programy natomiast mogą też wykorzystywać narzędzia do cyklicznego robienia zrzutów ekranu lub technologii VNC/RDP, czyli zdalnego podglądu pulpitu. Sposobów na monitorowanie pracowników jest naprawdę wiele, ale nie zawsze są one zgodne z prawem.

Warto pamiętać, że choć zakres funkcjonalności oprogramowania monitorującego może nie naruszać żadnych przepisów prawnych, wdrożenie monitoringu na szeroką skalę może już być prawnie nieuzasadnione. Na przykład, na podstawie art. 22[3] §1 Kodeksu Pracy, monitoring poczty elektronicznej może mieć miejsce tylko wtedy, gdy jest niezbędny „do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy”.

Niemniej, taki monitoring nie może naruszać tajemnicy korespondencji lub innych dóbr osobistych pracownika, według §2. Kolejnym przykładem problematycznego monitorowania jest zdalny dostęp do pulpitu (bez wiedzy pracownika) lub korzystanie z oprogramowania do robienia cyklicznych zrzutów ekranu.

Choć teoretycznie (i według umowy) pracownik nie powinien sprawdzać prywatnej poczty na urządzeniu służbowym, istnieje szansa na to, że to zrobi, choćby poprzez zalogowanie się do jakiejś usługi, np. konta Google. Tutaj powstaje problem prawny, ponieważ pracodawca nie może kontrolować prywatnej skrzynki swojego pracownika. Tak więc odkrycie, że pracownik zalogował się do prywatnego maila może być prawnie uzasadnione, natomiast posiadanie zrzutu ekranu, w którym widać prywatną korespondencję – już nie.

Jak pokazują powyższe przykłady, zakres i legalność monitoringu jest naprawdę skomplikowany i wymaga indywidualnej ewaluacji w każdym przedsiębiorstwie. Oczywiście pozostaje też kwestia etyczności takich rozwiązań. Pracownicy raczej nie będą zachwyceni monitorowaniem ich pracy. Jeśli już się na to decydujemy, warto wypracować sensowny kompromis pomiędzy monitorowaniem bezpieczeństwa firmowych zasobów a prywatnością pracownika, oraz jasno informować o zakresie monitoringu.

Zadbajmy o bezpieczeństwo mobilne

Praca zdalna to nie tylko korzystanie z komputera z połączeniem VPN. To również komunikacja smartfonem, poprzez platformy do zarządzania projektami, komunikatory i systemy telekonferencyjne.

Dziś smartfony to tak naprawdę równouprawnione komputery w wersji mobilnej. Łatwy w obsłudze interfejs sprawia wrażenie narzędzia pomocniczego, a wcale tak nie jest: smartfony obsługują technologię VPN, posiadają przeglądarki i aplikacje CRM, mają dostęp do maila i mogą zalogować się praktycznie wszędzie tam, gdzie komputer.

Jednocześnie nie są to urządzenia bardziej odporne na wszelkiego rodzaju złośliwe oprogramowanie – wręcz przeciwnie, coraz częściej stają się celem hakerów. Nie bez powodu. Smartfony często są używane jako urządzenie do weryfikacji dwuetapowej, a czasami mają też dostęp do kilku skrzynek mailowych i systemu weryfikacji jednocześnie. Ponadto są wyposażone w wysokiej rozdzielczości aparaty, czułe mikrofony i towarzyszą nam praktycznie wszędzie, co tworzy z nich idealne narzędzie do pozyskiwania danych poufnych.

Proaktywną postawą jest zaakceptowanie faktu, że smartfony już teraz stanowią i będą stanowiły część naszej infrastruktury teleinformatycznej. Ich ergonomiczność i wydajność sprawia, że pracownicy korzystają z nich regularnie, niekoniecznie stosując się do procedur i wytycznych. Warto więc zainwestować czas i pieniądze w wykreowanie realistycznej polityki urządzeń mobilnych, w tym urządzeń BYOD (ang. Bring Your Own Device) oraz zaoferować pracownikom zestaw ergonomicznych i bezpiecznych narzędzi mobilnych, których będą używać z wyboru, a nie z przymusu.

Kreujmy kulturę bezpiecznego przetwarzania danych

Statystyka wskazuje, że technologia nas nie zawodzi. Według badań Canona z 2019 r., tylko 17% badanych naruszeń bezpieczeństwa było spowodowanych przez faktyczne obejście zabezpieczeń.

Błąd ludzki oraz celowe działania pracowników to powód ok. 55- 59% wszystkich incydentów cybernetycznych. Tu tkwi sedno problemu: niska świadomość zagrożeń oraz brak stosowania dobrych praktyk podczas pracy z danymi co roku powodują ogromne straty w świecie biznesu. Tymczasem nie ma technologicznego lekarstwa na obojętność lub brak wiedzy. Zostają tylko szkolenia.

Najlepszą proaktywną postawą jest inwestycja w wiedzę pracowników, szczególnie tych pracujących zdalnie. Szkolenie powinno być kompleksowe, ponieważ muszą być oni świadomi tego, jak dochodzi do wycieków danych, jakie są konsekwencje dla całej firmy, oraz jaką rolę osobiście odgrywają w utrzymywaniu bezpieczeństwa danych.

Poza dobrymi praktykami, warto jest omówić też socjotechnikę, czyli manipulacje psychologiczne mające na celu przekonanie ofiary, aby zrobiła to, co chce haker. Edukujmy czym jest socjotechnika, jak ją rozpoznać i co zrobić, gdy podejrzewamy podstęp. Istotne jest, żeby pracownik był świadomy i nie podejmował pochopnych decyzji w momencie ataku.

„Technologia to jedno. Drugim jest zdrowy rozsądek, niezbędny, aby z niej korzystać. Zamiast kontrolować pracowników, lepiej jest zadbać o ich edukację w zakresie cyberbezpieczeństwa. Świadomy zagrożeń (oraz ich konsekwencji!) pracownik to dla

hakera twardy orzech do zgryzienia. Warto zainwestować w szkolenie z obrony przed atakami socjotechnicznymi lub (jeśli nie mamy środków na pomoc specjalistów) spróbować chociaż edukować na własną rękę" – mówi Tomasz Szpikowski, CEO TestArmy.

Kilka słów na koniec

Czas dostosować się do realiów, dopóki nie zaskoczą nas jeszcze bardziej. Przygotowanie kadry pracowniczej do pracy zdalnej może okazać się kluczem do utrzymania ciągłości biznesu na wypadek powrotu restrykcji związanych z koronawirusem lub nawet zwykłej zmiany preferencji pracowników.

Warto pamiętać też, że niektórych tendencji nie zahamujemy. Od dekady znany jest fakt, że to człowiek stanowi najsłabsze ogniwo w dziedzinie cyberbezpieczeństwa. Jednocześnie liczba osób wykonujących swoją pracę zdalnie z roku na rok rośnie, nawet jeśli nie jest napędzana impetem typowym dla pandemii. Warto zmierzyć się z tym problemem już teraz, aby w przyszłości nie zostać bohaterem powiedzenia „mądry Polak po szkodzie".