BEZPIECZEŃSTWO FIRMOWYCH URZĄDZEŃ RÓWNIEŻ PO PRACY. "WIĘKSZA PRODUKTYWNOŚĆ I OCHRONA"

„Problemem są nie tylko dane na urządzeniu, ale także podatność na występowanie trojana, którą można stworzyć w infrastrukturze korporacyjnej. Dlatego potrzebne są sprawdzone narzędzia, zapewniające najwyższy poziom bezpieczeństwa” – mówi CyberDefence24.pl Oleg Orlov, dyrektor regionalny w BlackBerry. Przedstawiciel firmy opowiada także o narzędziu BlackBerry Unified Endpoint Management, które umożliwia bezpieczną pracę zdalną.

CyberDefence24.pl: Firmy i organizacje często chcą zaoszczędzić na wydatkach związanych z cyberbezpieczeństwem, narażając się na atak, który w efekcie może kosztować je kilkaset razy więcej niż zakup skutecznego oprogramowania czy systemu do zarządzania urządzeniami. Jak przekonać je, że lepszym rozwiązaniem jest ochrona niż późniejsze likwidowanie skutków incydentu?

Oleg Orlov, dyrektor regionalny w BlackBerry: Często pojawia się brak zrozumienia na poziomie decyzyjnym w organizacji. Jak przekonać kogoś do ubezpieczenia samochodu lub domu? Każdego roku pojawia się 100 milionów przypadków nowego złośliwego oprogramowania, 60 proc. organizacji jest celem ataków, a nowa próba włamania następuje co 39 sekund. Z punktu widzenia prawdopodobieństwa, to zatem znacznie większe ryzyko niż wypadek samochodowy czy pożar domu.

Jeśli chodzi o przykłady „sukcesów” ataków ransomware, można łatwo je znaleźć. To m.in. przypadek Colonial Pipeline (wypłata okupu w wysokości 4 mln dolarów), Kaseya (ponad tysiąc dotkniętych firm i 800 supermarketów w Norwegii zamkniętych przez kilka dni), Accenture... I mówimy tylko o 2021 roku. Trzeba pamiętać, że najbardziej wyrafinowane ataki są przypisywane aktorom sponsorowanym przez państwo, takim jak Rosja. Polska musi być na nie dobrze przygotowana zarówno w sektorze prywatnym, jak i rządowym.

Fot. Oleg Orlov/ archiwum prywatne

Istotna z punktu widzenia organizacji czy instytucji jest także ochrona urządzeń końcowych, takich jak np. smartfony, tablety i komputery. Czy widać zmianę w myśleniu firm w tej kwestii?

Przedsiębiorstwa zdecydowanie mają świadomość i potrzebę ochrony, jednak podejście i oczekiwania są bardzo zróżnicowane. Większość mobilnych punktów końcowych to smartfony oraz tablety i tu mamy do czynienia z BYOD (ang. Bring Your Own Device; polityka firmy: „przynieść własne urządzenie do pracy" – red.). BYOD jest najbardziej wrażliwy i trudny do ochrony! Problemem są nie tylko dane na urządzeniu, ale także podatność na występowanie trojana, którą można stworzyć w infrastrukturze korporacyjnej. Dlatego potrzebne są sprawdzone narzędzia, zapewniające najwyższy poziom bezpieczeństwa.

Oferujecie narzędzie BlackBerry Unified Endpoint Management, które daje możliwość zarządzania całą flotą urządzeń końcowych, takich jak smartfony, tablety i komputery w firmie lub instytucji. Na czym dokładnie polega to rozwiązanie?

To system z oprogramowaniem na urządzeniu oraz możliwością korzystania z serwerów korporacyjnych, który zapewnia użyteczność dla najpopularniejszych aplikacji biznesowych (poczta e-mail, kalendarz, przeglądarka intranetowa) oraz tysięcy aplikacji korporacyjnych.

Większa mobilność pracowników - większa wydajność

Jakie zalety przynosi korzystanie z niego?

Gdy zapewniony jest bezpieczny dostęp do zasobów korporacyjnych, firma nie zmarnuje korzyści związanych ze zwiększoną mobilnością, a przy lepszej mobilności pracowników będzie mogła cieszyć się także większą wydajnością. Nastąpi zdecydowana zamiana „bezczynnego" czasu pracy na bardziej produktywny, przy wzroście o godzinę dziennie; nastąpi wzrost wydajności pracy o 10 proc. oraz możliwość natychmiastowego działania w oparciu o wrażliwe dane. Ma to wpływ na zwrot z inwestycji w firmie, jej wyniki, konkurencyjność oraz satysfakcję pracowników.

Jakie certyfikaty bezpieczeństwa posiada BlackBerry Unified Endpoint Management?

Mamy najlepsze certyfikaty bezpieczeństwa w branży ze strony: NATO, NIAP (National Information Assurance Partnership), certyfikat Common Criteria (EAL4+ Norwegia - poziom uzasadnionego zaufania do zabezpieczeń – red.), Agencji Bezpieczeństwa Narodowego USA, Departamentu Obrony Stanów Zjednoczonych.

Jak wygląda zarządzanie systemem BlackBerry UEM? Kto może z niego korzystać? Dla kogo jest przeznaczony: dla małych, średnich czy raczej wielkich korporacji?

System zarządzania UEM jest przyjazny i odpowiedni zarówno dla doświadczonych, jak i nowych administratorów mobilnych. Instalację na urządzeniu użytkownika końcowego można przeprowadzić bezpiecznie i samodzielnie. UEM może być zainstalowany na infrastrukturze klienta, w chmurze lub hybrydowo. Dlatego jest odpowiedni dla wszystkich rodzajów organizacji: przedsiębiorstw, przedstawicieli administracji rządowej oraz dla sektora małych i średnich przedsiębiorstw.

W Polsce mamy klientów z branży bankowej, produkcyjnej, rządowej. Kancelarie są dobrym przykładem małej organizacji, często około 10-osobowych. Jedna z nich wybrała BlackBerry UEM Cloud ze względu na maksymalne bezpieczeństwo przy bardzo ograniczonych zasobach w dziale IT.

Efekt pandemii

Rok 2020 oraz 2021 pokazał powszechność pracy zdalnej, często to pracownicy byli najsłabszych ogniwem w organizacjach i celem cyberataku. Czy BlackBerry Unified Endpoint Management pozwala na bezpieczne zarządzanie i ochronę urządzeń końcowych również poza biurem?

Na ochronę urządzeń mobilnych z systemem IOS czy Android – z definicji. Robimy także więcej niż konkurencja w zakresie zdalnej pracy na prywatnych laptopach z Windows 10 i czy na macOS. Wiele organizacji stanęło i stoi przed dylematem zakupu większej liczby korporacyjnych laptopów, zabezpieczenia urządzeń odpowiednim oprogramowaniem czy korzystaniem z koncentratorów VPN. To bardzo kosztowny skutek pandemii, zważając na fakt, że w wielu przypadkach biznesy borykały się z problemami. BlackBerry UEM oferuje prosty, opłacalny sposób na umożliwienie laptopom do zdalnej pracy bezpieczny dostęp do intranetu, z pełną ochroną danych w trakcie ich przesyłania, jak i w trakcie spoczynku urządzenia. Nie jest potrzebny VPN.

Jak w tym przypadku wygląda kwestia poniesionych kosztów na zarządzanie całą flotą urządzeń końcowych w stosunku do kosztów występowania potencjalnego

cyberzagrożenia?

Według danych IBM w 2021 roku zanotowano najwyższy średni wskaźnik kosztów naruszeń systemów od 17 lat i wyniósł on 4,24 mln dolarów. Kluczem jest słowo „średni". W wielu przypadkach naruszenie cyberbezpieczeństwa może doprowadzić do upadku całej firmy lub spowodować poważny incydent w krajowej infrastrukturze krytycznej. Zabezpieczenie wszystkich urządzeń użytkownika końcowego (smartfon, tablet, laptop) kosztuje mniej niż 100 dolarów rocznie w przeliczeniu na pracownika. Istotnym jest, by pamiętać, że BlackBerry UEM nie tylko chroni przed kosztownymi naruszeniami, ale zapewnia także znaczny wzrost produktywności firmy i pozytywnie wpływa na działalność finansową firmy.

Prognozując na kolejne 2-3 lata czy popularność tego typu rozwiązań będzie rosła?

Absolutnie.

Dziękuję za rozmowę.

Materiał powstał we współpracy z firmą BlackBerry.

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.