aut. Andrzej Kozłowski 24.02.2020

ZADBAJMY O BEZPIECZEŃSTWO SŁUŻBOWYCH SMARTFONÓW. EKSPERCI OSTRZEGAJĄ PRZED CYBERATAKAMI

Rośnie liczba cyberataków skierowanych na służbowe smartfony. Niestety firmy w Polsce są na to nieprzygotowane i w sposób zdecydowanie niewystarczający zabezpieczają służbowe telefony komórkowe – to główny wniosek płynący z raportu T-Mobile o bezpieczeństwie służbowych telefonów komórkowych przygotowanego wspólnie z firmą analityczno-badawczą PMR.

Dane zawarte w raporcie wskazują, że:

- 8 na 10 dużych przedsiębiorstw nie posiada oddzielnego budżetu na cyberochronę służbowych telefonów komórkowych. Wśród średnich firm odsetek ten sięga 100 %;
- 23% firm średniej wielkości i 10 % dużych nie posiada w swoich strukturach żadnej jednostki odpowiedzialne za bezpieczeństwo służbowych telefonów;
- 3/4 pracowników łączy się z publicznym Wi-Fi przez firmową komórkę;
- 27% średnich firm w Polsce nie stosuje żadnych zabezpieczeń w służbowych telefonach komórkowych.

Telefony komórkowe są nieodłącznym elementem funkcjonowania przedsiębiorstwa, wpływając na jego optymalizację kosztową i powodzenie prowadzonego biznesu.

PMR szacuje, że w 2018 r. liczba kart SIM w przedsiębiorstwach w Polsce wzrosła o 6%, osiągając poziom 10 mln sztuk. Rosnąca baza kart SIM wykorzystywanych przez klientów biznesowych jest pochodną zwiększającej się liczby podmiotów biznesowych i pracowników oraz rozwoju gospodarki.

Telefony coraz częstszym celem ataków

Dane oraz połączenia smartfonów z aplikacjami firmowymi jak skrzynka mailowa, komunikatory powoduje, że stają się one naturalnym celem dla cyberprzestępców.

Zainteresowanie ze strony cyberprzestępców potwierdza fakt szukania podatności bezpośrednio na kartach SIM, aby w ten sposób przejąć kontrolę nad urządzeniem użytkownika – piszą autorzy raportu. Smartfony w przeciwieństwie do komputerów aktywne są praktycznie przez całą dobę, co ułatwia działanie hakerów. Wpływa na to również fakt, że telefonów jest obecnie wielokrotnie więcej niż wszystkich komputerów w firmie. 6% pracowników działu IT w średnich i dużych przedsiębiorstwach podejrzewa, że w ich organizacji w ciągu ostatniego roku co najmniej jeden pracownik padł ofiarą cyberataku na służbowy telefon komórkowy. Podejrzenia pracowników zespołów IT różnią się od deklaracji użytkowników, którzy w zdecydowanej większości nie przypominają sobie wystąpienia sytuacji związanej z naruszeniem cyberbezpieczeństwa służbowego telefonu. Dane z systemu Cyber Guard T-Mobile Polska pokazują jednak, że takie incydenty mają faktycznie miejsce. Autorzy

zauważają, że zdecydowanie większy odsetek pracowników działów IT podejrzewa wystąpienie cyberataku na firmowe telefony niż wynikałoby to z deklaracji ich użytkowników. Ich zdaniem różnica ta może wynikać z obaw pracowników co do przyznawania się do naruszenia cyberbezpieczeństwa na ich służbowych telefonach. Trudno jest jednak określić prawdziwą liczbę incydentów, ponieważ aż 43 % polskich firm nie prowadzi takich rejestrów.

Nieostrożne przedsiębiorstwa

Zarządzający wydają się nie dostrzegać dynamicznych zmian zachodzących na rynku w wykorzystaniu smartfonów – czytamy w raporcie. Dla rosnącej liczby pracowników smartfon to obecnie drugi komputer i podstawowe narzędzie pracy, z którego 98% zatrudnionych korzysta codziennie. Pomimo tego, firmy praktycznie nie wydzielają osobnego budżetu na zabezpieczanie służbowych telefonów. Stosowane przez nich narzędzia zabezpieczające są proste i nadal w ogromnej większości poprzestają na zabezpieczaniu ekranu, co robi trzy czwarte dużych firm w Polsce oraz instalacji oprogramowania antywirusowego. W praktyce ten rodzaj zabezpieczenia może wymuszać producent urządzenia lub dostawca oprogramowania, a nie zawsze jest to świadoma polityka organizacji – czytamy w raporcie. Pracownicy aż 27% średnich firm w Polsce w ogóle nie zabezpieczało swoich firmowych komórek, czyli taki sprzęt de facto może być używany przez dowolna osobę z zewnątrz.

Jedynym z problemów jest instytucjonalna odpowiedzialność za cyberbezpieczeństwo telefonów komórkowych. W części przedsiębiorstw obowiązek nadzoru nad bezpieczeństwem firmowych komórek spoczywa na dziale administracji – takie podejście ma aż co szósta średnia organizacja w naszym kraju. Oznacza to marginalizację problemu, ponieważ trudno jest oczekiwać, żeby dział administracji posiadał odpowiednią wiedzę odnośnie bezpieczeństwa teleinformatycznego – twierdzą autorzy raportu. Najbardziej szokujące są jednak dane o braku w swoich strukturach podmiotu odpowiedzialnego za bezpieczeństwo służbowych telefonów komórkowych, co deklaruje aż 23 % średnich i 10 % dużych firm.

Badania wskazują również na rozdźwięk pomiędzy oceną jednostek IT, a faktycznym użytkowaniem smartfonów przez użytkowników końcowych. W ocenie ekspertów IT tylko co dziesiąty pracownik wykorzystuje telefon do obsługi prywatnej poczty, podczas gdy z perspektywy użytkowników sprzętu jest to jeden z głównych obszarów zastosowania firmowego smartfona. W przypadku dużych przedsiębiorstw, blisko co druga osoba (47%) używa telefonu w tym celu. Podobny rozdźwięk występuje w przypadku hotspotów. Dwie trzecie działów IT deklaruje, że służbowe telefony nie mogą się łączyć w ten sposób z Internetem, ale w praktyce tylko 4% przedsiębiorstw technicznie blokuje taką możliwość. W efekcie trzy czwarte pracowników łączy się z publicznym Wi-Fi przez firmową komórkę. Skorzystanie z otwartego Wi-Fi to wprawdzie tylko ekspozycja na ryzyko, a nie natychmiastowa utrata danych czy nieautoryzowany dostęp do firmowych zasobów, ale problemu tego nie należy lekceważyć. Są to o tyle niebezpieczne sytuacje, że usypiają czujność firmy i tworzą fałszywe przeświadczenie, że poziom ryzyka jest niski. Autorzy raporty konkludują, że gdyby przedsiębiorstwa realnie oceniły skalę zjawiska, z pewnością zmieniłoby się ich podejście do inwestycji w profesjonalne zabezpieczenie firmowych telefonów i kompleksową politykę w tym zakresie.

Dyrektor Departamentu Bezpieczeństwa T-Mobile Polska Paweł Dobrzański podkreślił, że firmy w dalszym ciągu zbyt mało uwagi poświęcają zagadnieniu cyberbezpieczeństwa telefonów służbowych. Według eksperta T-Mobile firmy powinny:

- Przydzielić odpowiedzialność za bezpieczeństwo smartfonów konkretnej jednostce;
- Stworzyć kompleksową politykę użytkowania takiego sprzętu;
- Dobrać odpowiednie narzędzia bezpieczeństwa oraz skutecznie nimi zarządzać;
- Wdrożyć monitoring urządzeń;
- Rozważyć zasięgnięcie rady partnerów zewnętrznych.

T-Mobile Polska od lat konsekwentnie angażuje się w budowanie świadomości przedsiębiorstw w tym zakresie. Te działania skutkują oczywiście również ciągłym tworzeniem i doskonaleniem adekwatnych produktów. Do takich rozwiązań należy autorska usługa T-Mobile o nazwie Cyber Guard, która analizuje cały ruch w sieci (kilkanaście miliardów sesji internetowych dziennie) – bazując na szerszych danych niż tylko DNS – pod kątem zdefiniowanych zagrożeń, dopasowanych profilem do potrzeb firmy. Oprogramowanie pozwala na zdefiniowanie indywidualnych blokad bezpieczeństwa, wybranych pod kątem organizacji. Umożliwia to sprawne zarządzanie bezpieczeństwem wszystkich firmowych mobilnych urządzeń, dzięki czemu wychwytywanie incydentów jest dużo łatwiejsze. Warto podkreślić, że technologia ta pozwala nie tylko ochronić się przed cyberzagrożeniami, w tym wyciekami danych, ale również przed nadużyciami, co pozostaje równie istotną kwestią dla bezpieczeństwa całej firmy.

Raport „Badania rynku bezpieczeństwa służbowych telefonów komórkowych w Polsce w 2019 roku" przygotowany został przez T-Mobile, miał na celu pokazanie stanu zabezpieczeń firmowych telefonów komórkowych w polskich przedsiębiorstwach. Badanie zostało przeprowadzone z punktu widzenia firm, użytkowników oraz operatorów sieci. Są to pierwsze badania na poziomie B2B, dodatkowo skonfrontowane ze statystykami T-Mobile Polska.

Raport można pobrać stąd

Materiał powstał we współpracy z T-Mobile Polska