Bitdefender

Rozwikłanie głównych wyzwań związanych z bezpieczeństwem urządzeń mobilnych w pracy zdalnej

09.08.2023

Firmy i organizacje coraz częściej znajdują się w ciągłym przeciąganiu liny z cyberprzestępcami na wielu frontach. Od walki z szeregiem zagrożeń i łagodzenia słabych punktów, po zarządzanie ryzykiem związanym ze środowiskami opartymi na chmurze i zewnętrznymi dostawcami. Ponadto istnieje jeden wektor ataków, któremu nie poświęca się należytej uwagi – zwłaszcza biorąc pod uwagę post-pandemiczny świat, w którym żyjemy – bezpieczeństwo mobilne. Urządzenia mobilne, często uważane za peryferyjne komponenty cyberbezpieczeństwa przedsiębiorstwa, ewoluowały i stały się centralnym elementem operacji, a co za tym idzie, stały się atrakcyjnym celem dla cyberprzestępców. Dlatego zespół Bitdefender przygotował poradnik dla przedsiębiorców, dzięki któremu będą mogli podnieść poziom bezpieczeństwa urządzeń mobilnych wykorzystywanych w firmie.

Zagrożenia dla bezpieczeństwa urządzeń mobilnych

Pomimo rosnącego zagrożenia wiele organizacji ma tendencję do pomijania znaczenia bezpieczeństwa mobilnego w ogólnej strategii bezpieczeństwa. Większość firm albo ignoruje zabezpieczenia urządzeń mobilnych, albo uważa, że rozwiązania do zarządzania urządzeniami będą wystarczające, zamiast skupiać się na samych zagrożeniach bezpieczeństwa urządzeń mobilnych. Być może dlatego złośliwe oprogramowanie skierowane na smartfony i tablety są jednymi z najszybciej rozwijających się rodzajów cyberzagrożeń. Badania przeprowadzone przez firmę Zimperium wykazały, że 80% stron phishingowych jest skierowanych na urządzenia mobilne lub zaprojektowanych tak, aby działały zarówno na urządzeniach mobilnych, jak i na komputerach stacjonarnych.

Krajobraz zagrożeń mobilnych

Pandemia znacznie zintensyfikowała korzystanie z urządzeń mobilnych, zarówno osobistych, jak i tych, które są przeznaczone do pracy zdalnej. Ponad 60% respondentów podczas badania siły roboczej, w którym wzięło udział ponad 1500 osób, stwierdziło, że urządzenia mobilne odgrywają kluczową rolę w ich wydajności pracy. Jednak wzrost ten niesie ze sobą również gwałtowny rozwój związanych z nim zagrożeń bezpieczeństwa.

Pracownicy mogą nie zdawać sobie sprawy z podwyższonego ryzyka, jakie stwarzają, korzystając z własnych urządzeń w nieautoryzowanych sieciach. Na przykład istnieje powszechne błędne przekonanie, że

urządzenia z systemem iOS są z natury bezpieczne, co może powodować, że użytkownicy wykonują na nich jeszcze bardziej ryzykowne działania. W sklepie Apple App Store znaleziono wiele aplikacji, które zostały oznaczone jako złośliwe, a także wykryto wiele luk zero-day skierowanych do aplikacji na iOS.

Wiadomości e-mail są nadal głównym nośnikiem wielu ataków i nie inaczej jest w przypadku urządzeń mobilnych. Hakerzy stale opracowują nowe techniki phishingu ukierunkowane na aplikacje i systemy mobilne, takie jak SMS (smishing), WhatsApp i media społecznościowe.

Organizacje powinny zacząć od bezpośredniego zajęcia się ochroną smartfonów i tabletów poza tradycyjnymi narzędziami do zarządzania urządzeniami mobilnymi (MDM). Narzędzia te zarządzają urządzeniami w sieci, co może być pomocne, ale takie rozwiązania nie eliminują bezpośrednio bardziej wyrafinowanych zagrożeń, ponieważ ich podstawową funkcją jest zarządzanie urządzeniami, a nie ich zabezpieczanie. Narzędzia do ochrony przed zagrożeniami mobilnymi (MTD) zostały zaprojektowane w celu proaktywnej ochrony mobilnych punktów końcowych przed znanymi atakami i zagrożeniami poprzez wykrywanie i usuwanie zagrożeń mobilnych, niezależnie od tego, czy są to aplikacje, złośliwe oprogramowanie systemu operacyjnego, czy ataki sieciowe skierowane na urządzenia mobilne.

Odkrywanie ukrytych zagrożeń w zabezpieczeniach mobilnych

Ponieważ organizacje zmagają się z wyzwaniami związanymi z bezpieczeństwem urządzeń mobilnych, niezwykle ważne jest dogłębne

zrozumienie konkretnych zagrożeń, z którymi się borykają.

Luki w oprogramowaniu i systemach

Hakerzy próbują znaleźć luki w zabezpieczeniach platformy iOS lub Android, aby wykorzystać przestarzałą aplikację do naruszenia bezpieczeństwa systemu. Aby chronić się przed tymi zagrożeniami, warto korzystać z systemu zarządzania lukami, a także wymagać polityki automatycznych aktualizacji oprogramowania i aktualizacji systemu od swoich pracowników.

Złośliwe aplikacje

Złośliwe aplikacje istnieją prawie tak długo, jak urządzenia, które są ich celem. Te aplikacje – jeśli zostały pobrane poza oficjalnym sklepem z aplikacjami – często wiążą się z większym ryzykiem bycia złośliwym, nawet jeśli oprogramowanie jest legalne. Nawet gdy korzystamy tylko ze sklepów z aplikacjami, to nadal grozi nam niebezpieczeństwo pobrania złośliwej aplikacji. Podczas gdy Google i Apple rzekomo dokładnie sprawdzają wszystkie programy, które trafiają na ich platformy, to wiele złośliwych wersji przedostaje się na miliony urządzeń mobilnych. W niektórych przypadkach wystarczy prosta zmiana nazwy, aby niebezpieczna aplikacja wróciła do Sklepu Play.

Urządzenie mobilne jako wektor

„Wiele prób włamania się lub zaatakowania systemu odbywa się za pośrednictwem urządzenia mobilnego. Hakerzy robią to za pomocą

phishingu tekstowego (smishing), umieszczania złośliwych reklam w legalnych aplikacjach lub znajdowania sposobów na złamanie zabezpieczeń urządzenia za pośrednictwem poczty e-mail, mediów społecznościowych, a także mobilnego oprogramowania ransomware" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Pomimo powagi tych zagrożeń, wiele organizacji nadal nie nadaje priorytetu bezpieczeństwu urządzeń mobilnych. Zespołom do spraw cyberbezpieczeństwa często brakuje wiedzy na temat skutecznego zabezpieczania tych urządzeń lub procesów i infrastruktury wspierających solidne zabezpieczenia mobilne. Ten brak priorytetu oraz gotowości stwarza okazje do wykorzystania przez atakujących.

Jak organizacje mogą zabezpieczyć swoje urządzenia mobilne?

Organizacje powinny wdrożyć solidne środki bezpieczeństwa, które dotyczą w szczególności bezpieczeństwa mobilnego. Można to zrobić za pomocą kombinacji zasad, procesów i kluczowych rozwiązań do ochrony przed zagrożeniami mobilnymi. Ten typ rozwiązania różni się od zarządzania urządzeniami mobilnymi (MDM) i bezpośrednio eliminuje zagrożenia, a nie tylko zarządza urządzeniami mobilnymi. Poszukując skutecznego rozwiązania MTD, organizacje powinny nadać priorytet następującym kwestiom.

Ochrona przed złośliwymi aplikacjami: kompleksowa strategia bezpieczeństwa mobilnego powinna obejmować funkcje sprawdzania aplikacji i chronić je nie tylko przed znanymi złośliwymi aplikacjami, ale

także przed niebezpiecznymi aplikacjami, które mogą potencjalnie prowadzić do problemów ze zgodnością.

Łagodzenie ataków sieciowych: urządzenia mobilne są częstymi celami ataków sieciowych, dlatego skuteczne rozwiązanie powinno skupiać się na identyfikowaniu i neutralizowaniu takich zagrożeń.

Ochrona sieci Web/phishing: biorąc pod uwagę powszechność zagrożeń typu phishing skierowanych na urządzenia mobilne, ochrona sieci jest niezbędnym elementem kompleksowej strategii bezpieczeństwa urządzeń mobilnych.

Bieżące ograniczanie ryzyka i zagrożeń: atakujący działają szybko, więc posiadanie rozwiązania proaktywnego przeciwko potencjalnym zagrożeniom dnia zerowego i nowo odkrytym lukom w zabezpieczeniach może pomóc organizacjom wyprzedzić atakujących.

Bezpieczeństwo urządzeń mobilnych powinno być istotnym elementem każdej strategii bezpieczeństwa cybernetycznego, a liderzy powinni zrozumieć, że partnerstwo z dostawcą doprowadzi do szybszego wdrożenia cyberbezpieczeństwa i skuteczniejszego zwalczania zagrożeń.

Źródło:https://bitdefender.pl/rozwiklanie-glownych-wyzwan-zwiazanych-z-bezpieczenstwem-urzadzen-mobilnych-w-pracy-zdalnej/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 09.08.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.