



Twoi pracownicy to mobilny cel hakerów wizualnych

Napisane przez Luizę Dzienkiewicz-Kobus



Dowiedz się więcej



Dzięki HP Sure View zabezpieczysz ekrany swoich firmowych urządzeń przed wścibskimi oczami.

Nie wszyscy hakerzy powstałi tak samo. Podczas gdy firmy wzmacniają ochronę przed zaawansowanymi cyberatakami, wiele z nich zapomina o zachowaniu czujności, jeśli chodzi o zagrożenia o małym stopniu zaawansowania technologicznego – takie jak wizualne ataki hakerskie.

Do wizualnego ataku hakerskiego dochodzi, gdy „szpiedzy patrzący przez ramię” sprawdzają, co znajduje się na ekranach komputerów i biurkach innych osób oraz uzyskują informacje niejawne, aby wykorzystać je w niedozwolony sposób. Uznano go za piąte najbardziej niedostrzegane zagrożenie o małym stopniu zaawansowania technologicznego, ponieważ w jego przypadku nie są pozostawiane żadne ślady i często pozostaje ono niezauważone przez informatyków. Ofiarą takiego ataku może paść każdy w każdym miejscu i o każdej porze. Wywołuje on natychmiastowe i nieodwracalne konsekwencje.

W ramach [eksperymentu](#) przeprowadzonego przez Ponemon Institute okazało się, że 91% wizualnych prób ataków hakerskich zakończyło się powodzeniem, a 52% przechwyconych informacji wrażliwych pochodziło z ekranów komputerów pracowników¹. Statystyki te potrafią wyprowadzić z równowagi, biorąc pod uwagę fakt, że ataki te mogą wiązać się z takimi szkodliwymi konsekwencjami, jak naruszenie bezpieczeństwa sieci – począwszy od kradzieży danych logowania użytkowników, a skończywszy na kradzieży poufnych informacji o klientach.

Gdyby dane te dostały się w niepowołane ręce, zaufanie i pewność Twoich klientów mogłyby zostać zachwiane, co zaszkodziłoby przyszłości Twojej firmy.

Pilnowanie, aby pracownicy zabezpieczali poufne dane firmowe powinno być priorytetem firm, zwłaszcza w obliczu zwiększającego się zakresu pracy wykonywanej zdalnie. Dzisiejsi pracownicy nie boją się wykorzystywać technologii mobilnych do maksimum, pracując w pociągu, wspólnej przestrzeni biurowej lub kawiarni, dzięki czemu mogą zabrać swoją pracę poza biuro. Jednak w takim przypadku mają oni mniej barier, za którymi mogą ukryć informacje cyfrowe. Zamiast tego pojawia się większe ryzyko, że osoby przechodzące obok pracowników zobaczą ekrany ich urządzeń, przez co pracownicy ci stają się potencjalnymi celami wizualnych ataków hakerskich, a wszystko razem sprawia, że Twoja firma zostaje narażona na niebezpieczeństwo.

Firmy nie mogą już pozwolić sobie na ignorowanie tego rosnącego zagrożenia o niskim stopniu zaawansowania technologicznego. Muszą one podejmować odpowiednie działania i podwoić środki zapewniające im bezpieczeństwo w cyberprzestrzeni. Oznacza to lepsze oprogramowanie, szkolenia w zakresie najlepszych praktyk związanych z bezpieczeństwem oraz urządzenia z wbudowanymi funkcjami zabezpieczającymi, takimi jak rozwiązanie [HP Sure View](#), dostępne na komputerach [HP EliteBook 800 Series](#) z opcjonalnym procesorem Intel® Core™ 8. generacji – są to najbezpieczniejsze na świecie i łatwe w zarządzaniu komputery².

Twoi pracownicy to mobilny cel hakerów wizualnych

HP Sure View to jedno z szeregu [rozwiązań firmy HP zapewniających bezpieczeństwo](#) i stanowi ono jedyny na świecie zintegrowany ekran komputera do ochrony prywatności³.

„Dodanie HP Sure View do naszych rozwiązań do ochrony komputerów [...] zapewnia klientom swobodę, dzięki której mogą oni pracować pewniej i wydajniej w przestrzeni publicznej, zabezpieczając się jedynie poprzez dotknięcie przycisku”.

-Alex Cho, Wiceprezes i Dyrektor Generalny HP ds. Komputerów Komercyjnych

Zadaniem tego narzędzia jest ograniczanie widocznego światła nawet o 95% po naciśnięciu odpowiedniego przycisku oraz uniemożliwianie hakerom wizualnym patrzenia na ekran z boku. Treść dostępną na ekranie widzą tylko użytkownicy patrzący na niego prosto, dzięki czemu, bez względu na to, gdzie pracujesz, możesz mieć pewność, że Twoje informacje są chronione i nie dostaną się w niepowołane ręce.

Jeżeli jednak chodzi o uzyskiwanie dostępu do najnowocześniejszych urządzeń – takich jak to – łatwiej jest to powiedzieć niż zrobić.

W tym przypadku można skorzystać z pomocy rozwiązań komputerowych, takich jak [HP Device as a Service \(DaaS\)](#). Jest to nowoczesny model korzystania z komputerów, który upraszcza sposób, w jaki organizacje komercyjne wyposażają swoich pracowników w odpowiedni sprzęt i akcesoria, zarządzają flotami urządzeń z różnymi systemami operacyjnymi i korzystają z dodatkowych usług w ramach cyklu życia tych urządzeń. W ramach HP DaaS dostępne są proste, a zarazem elastyczne plany oferowane w jednej cenie dla każdego urządzenia. Połączenie tego rozwiązania z urządzeniem, takim jak [HP EliteBook 800 Series](#), z opcjonalnym procesorem Intel® Core™ 8. generacji, może umożliwić firmie płynne i wydajne prowadzenie działalności.

Aby dowiedzieć się więcej na temat tego, jak chronić urządzenia w swojej firmie, przeczytaj nasze najnowsze [opracowanie dotyczące rozwiązania HP Sure View](#) i odkryj korzyści, jakie [rozwiązania zabezpieczające firmy HP](#) mogą zapewnić Twojej firmie.

Źródła:

1. <https://www.infosecurity-magazine.com/news/visual-hacking-is-successful-91-of/>
2. W oparciu o unikalne i wszechstronne funkcje zabezpieczeń HP bez dodatkowych kosztów oraz zarządzanie w ramach zestawu HP Manageability Integration Kit wszystkimi aspektami komputera, w tym sprzętem, BIOS-em oraz zarządzanie oprogramowaniem przy użyciu programu Microsoft System Center Configuration Manager, wśród dostawców z roczną sprzedażą na poziomie ponad 1 mln urządzeń (listopad 2016) w przypadku komputerów HP Elite z procesorami Intel® Core® 7. generacji, zintegrowaną grafiką Intel® i technologią Intel® WLAN.

© Copyright 2018 HP Development Company, L.P. Specyfikacje zawarte w tym dokumencie mogą ulec zmianie bez uprzedzenia.

4AA7-3171PLE, Może 2018 r.

