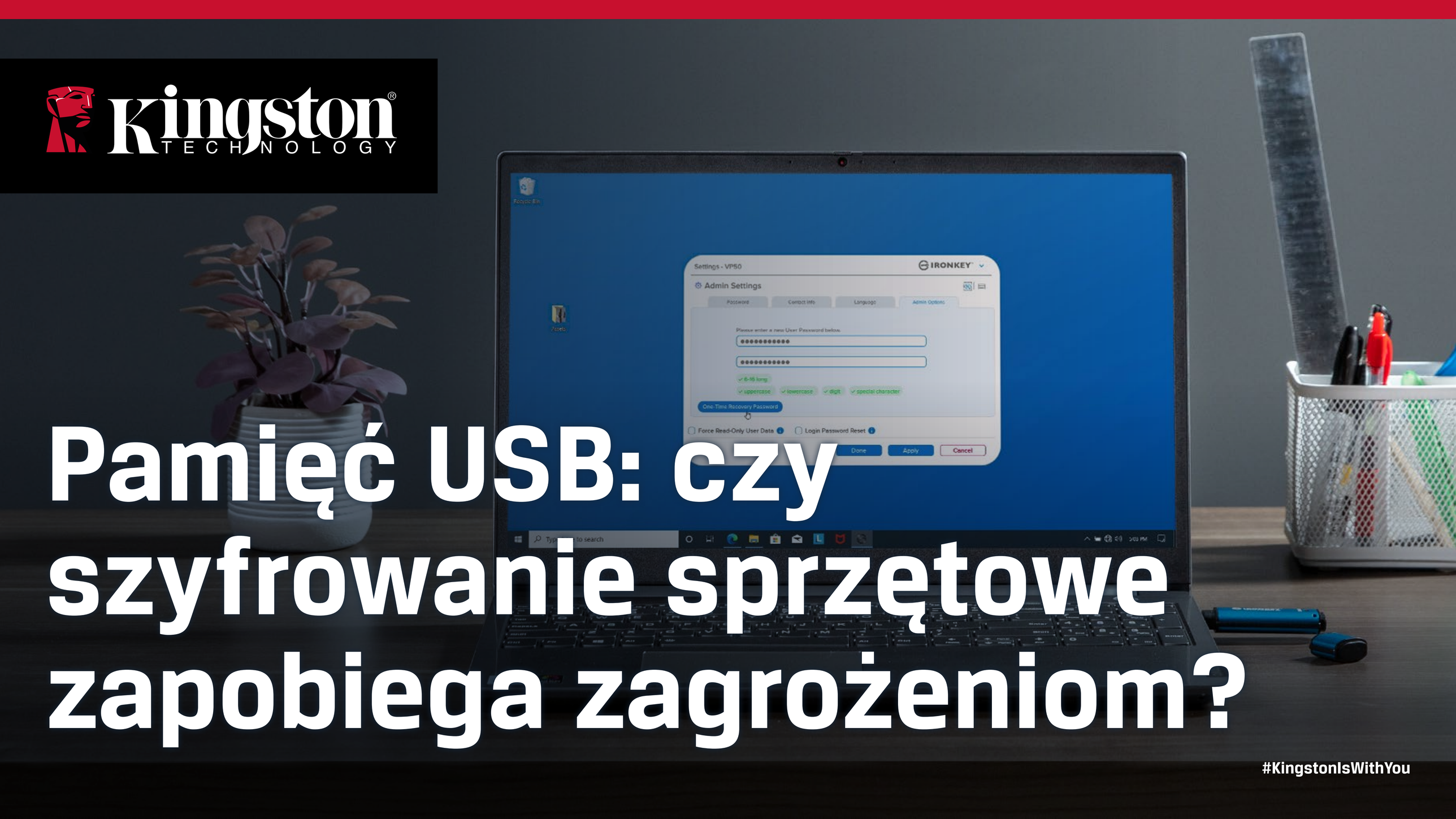

Kingston
TECHNOLOGY
Settings - VP50
IRONKEY
Admin Settings
Password
Contact Info
Language
Admin Options
Please enter a new User Password below.
6-16 long
uppercase
lowercase
digit
special character
One-Time Recovery Password
Force Read-Only User Data
Login Password Reset
Done
Apply
Cancel
Pamięć USB: czy szyfrowanie sprzętowe zapobiega zagrożeniom?
#KingstonIsWithYou

Pamięć USB: czy szyfrowanie sprzętowe zapobiega zagrożeniom?

Przedmowa i spis treści

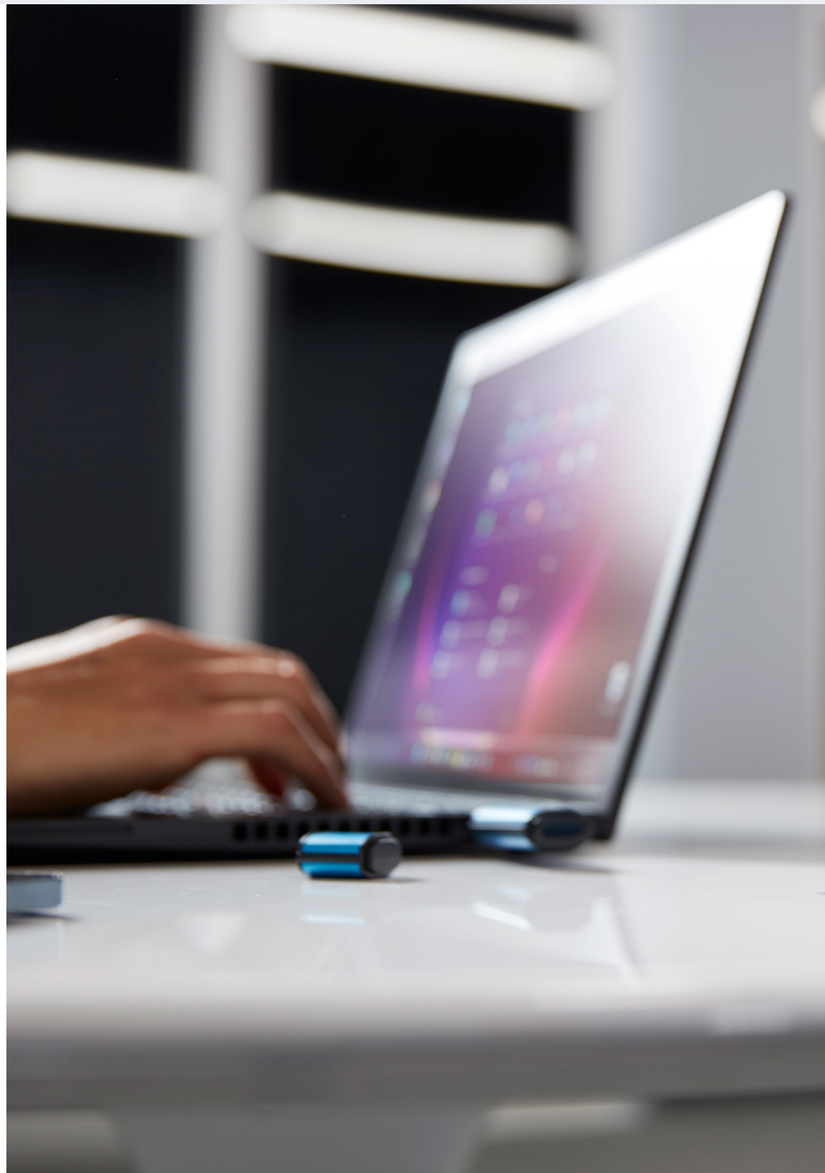
Cyberbezpieczeństwo jest większym problemem dla firm niż kiedykolwiek dotąd, jednak zbyt wiele organizacji jest niedoinformowanych i niedostatecznie przygotowanych na związane z tym zagrożenia. Według portalu UpCity tylko 50% firm w Stanach Zjednoczonych ma wdrożoną politykę zapewnienia cyberbezpieczeństwa, a 32% z nich nie zaktualizowało swoich planów od początku pandemii COVID-19, podczas której wiele organizacji przeszło na model pracy zdalnej lub hybrydowej. Tymczasem częstotliwość cyberataków rośnie – na całym świecie liczba firm dotkniętych atakami z wykorzystaniem oprogramowania ransomware wzrosła z 37% w 2020 r. do 66% w 2021 r[1].

Zagrożenia związane z naruszeniem cyberbezpieczeństwa mogą mieć niszczące skutki dla firmy. Koszty finansowe oraz utrata danych, bezpieczeństwa i reputacji wskutek cyberataków mogą mieć wielowymiarowy, krótko- i długoterminowy negatywny wpływ na organizację.

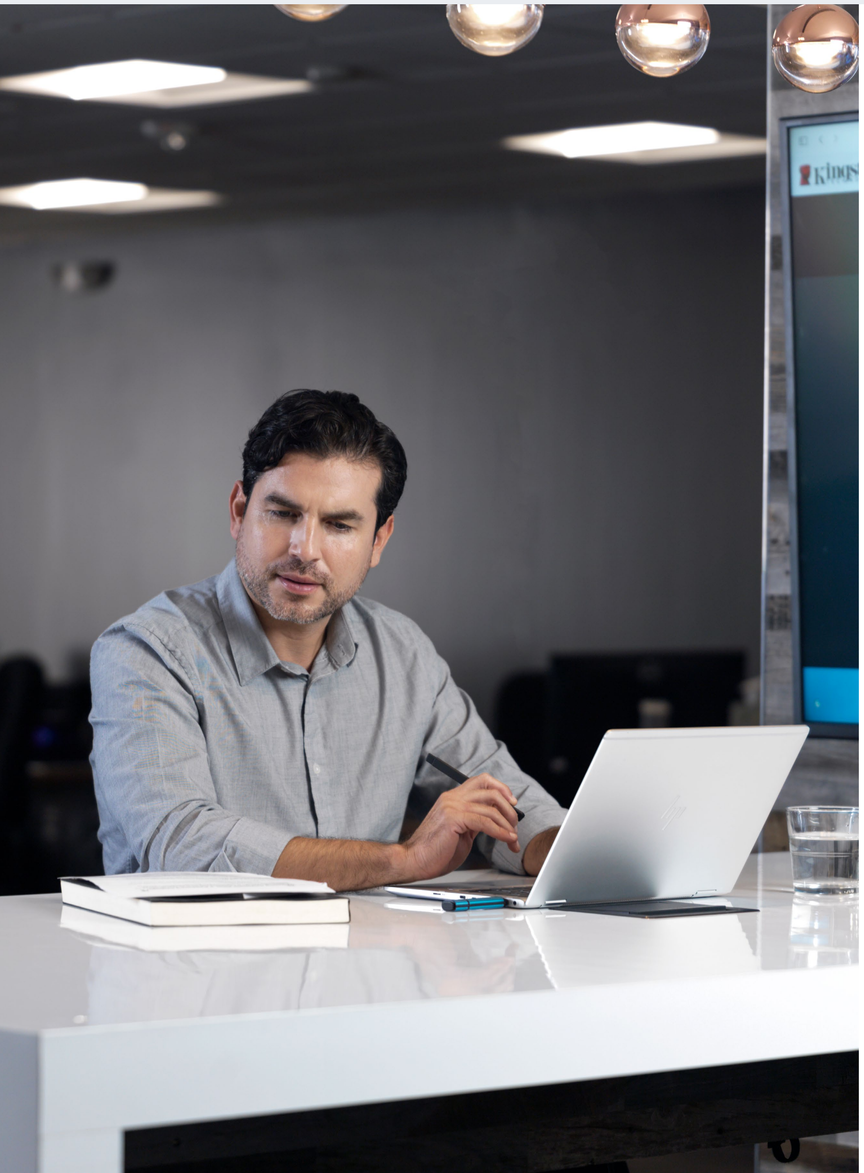
Jednym z powszechnie występujących źródeł zagrożeń są urządzenia pamięci USB. Są one wszechobecne w wielu organizacjach ze względu na ich prostotę – wystarczy podłączyć je do komputera i są gotowe do użycia. Jednak to właśnie prostota sprawia, że urządzenia pamięci USB są tak podatne na ataki: wystarczy jedna zgubiona lub skradziona pamięć, aby ktoś nieuczciwy uzyskał dostęp do potencjalnie wrażliwych danych. Właśnie w takich przypadkach szyfrowanie może odegrać znaczącą rolę w zapewnieniu bezpieczeństwa pamięci USB i ograniczeniu zagrożeń dla użytkowników i organizacji. W tym e-booku odpowiadamy na następujące ważne pytania:

- Dlaczego szyfrowana pamięć USB jest tak ważna w ochronie przed cyberatakami?
- Co czyni organizacje podatnymi na zagrożenia?
- Co mogą zrobić, aby się chronić?

Spis treści	Strony



Pamięć USB: czy szyfrowanie sprzętowe zapobiega zagrożeniom?



Autorzy

Opracowanie powstało z udziałem czołowych ekspertów z branży IT i nowych technologii oraz eksperta technicznego firmy Kingston.

David Clarke

David został uznany za jednego z 10 najbardziej wpływowych influencerów, którzy znaleźli się w rankingu Thomson Reuters „30 najbardziej wpływowych liderów opinii i intelektualistów w mediach społecznościowych w dziedzinie zarządzania ryzykiem, zapewnienia zgodności z przepisami i technologii regulacyjnych w Wielkiej Brytanii", a także trafił na listę 50 czołowych światowych ekspertów firmy Kingston Technology.

Pasi Siukonen

Pasi kieruje zespołem ekspertów współpracujących w zakresie rozwoju produktów Kingston z działami PR, marketingu, sprzedaży, pomocy technicznej i obsługi klienta firmy Kingston. Głównym przedmiotem jego zainteresowania są linie produktów pamięci flash i SSD.

Różnica między standardową a szyfrowaną pamięcią

Chociaż dostęp do standardowej (nieszyfrowanej) pamięci i korzystanie z niej jest niezwykle proste, szyfrowanie sprzętowe dodaje kilka warstw zabezpieczeń – zarówno fizycznych, jak i cyfrowych – dzięki czemu pamięć USB staje się znacznie bezpieczniejsza. Łatwa dostępność, niski koszt i przenośność standardowej, nieszyfrowanej pamięci oznacza, że chociaż jest ona bardzo wygodna w użyciu, jest taka również dla przestępców, których celem jest kradzież poufnych danych, wprowadzenie do firmowej sieci złośliwego oprogramowania lub oprogramowania ransomware itp. Ponieważ pamięci USB są często używane, daje wiele możliwości cyberataków. Istnieją dwa główne zagrożenia związane ze standardową pamięcią:

- **Ataki ransomware:** : te oparte na wykorzystaniu pamięci USB ataki polegają na wprowadzeniu złośliwego oprogramowania do sieci firmowych i zablokowaniu informacji lub systemów firmy poprzez ich zaszyfrowanie w celu uzyskania okupu. Są one często przeprowadzane z wykorzystaniem luki BadUSB i stały się najczęściej stosowaną metodą wykorzystania złośliwego oprogramowania.
- **Kradzież danych:** wystarczy zgubiona, skradziona lub pozostawiona bez nadzoru pamięć USB bez odpowiednich zabezpieczeń, aby ktoś nieuczciwy mógł łatwo uzyskać dostęp do przechowywanych w niej danych – informacji o klientach, kodu źródłowego, poufnych danych finansowych, wyników firmy itp.

BadUSB to rodzaj ataku, który wykorzystuje lukę w zabezpieczeniu oprogramowania sprzętowego pamięci USB w celu zainfekowania jej złośliwym oprogramowaniem. Te złośliwe narzędzia są bardzo rozpowszechnione i łatwo dostępne dla cyberprzestępców, natomiast świadomość ich istnienia wśród użytkowników wciąż pozostaje niska. Dlatego nadal zbyt łatwo można przeprowadzić atak polegający na zastąpieniu oprogramowania sprzętowego standardowej pamięci USB jego zhakowaną wersją, która może podszywać się pod klawiaturę i uruchamiać skrypty umożliwiające atak przez zaporę firewall. Ponieważ tak wiele cyberataków odbywa z udziałem będących poza podejrzeniami pracowników (niekoniecznie mających złe zamiary), bardzo ważne jest, aby firmy korzystały z szyfrowanych urządzeń pamięci. Są one wyposażone w zabezpieczone, podpisane cyfrowo oprogramowanie sprzętowe, które zapobiega tego typu atakom i zmniejsza szanse powodzenia działań cyberprzestępców.

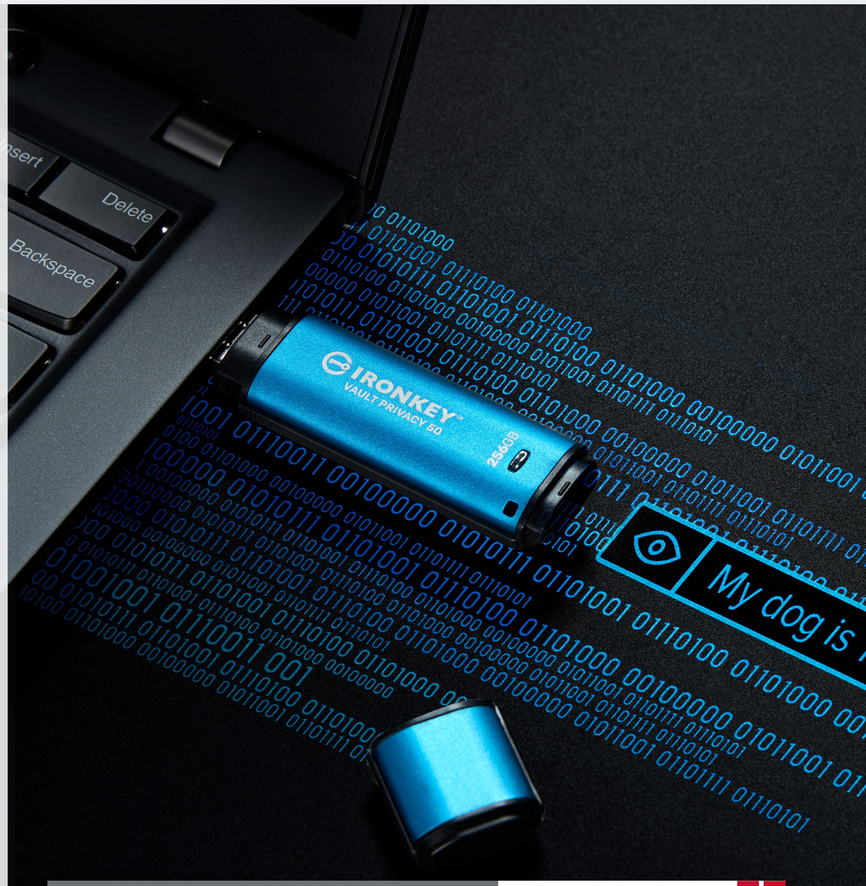
> **Koszty odbudowy infrastruktury, a także wynikające z konieczności zapłacenia okupu i innych wymuszeń, są ogromne w porównaniu z kosztami zakupu zarządzanej pamięci USB. - David Clarke**

Dlaczego warto korzystać z szyfrowanej pamięci USB?

Szyfrowane urządzenia pamięci są specjalnie zaprojektowane, aby chronić zapisane na nich dane, a także inne urządzenia, do których mogą zostać podłączone. Dzięki temu są cennymi narzędziami w arsenale IT każdej organizacji. Odpowiedzią na coraz bardziej zaawansowane zagrożenia związane z naruszeniem cyberbezpieczeństwa, są zaawansowane funkcje szyfrowanych urządzeń pamięci, pozwalające wyprzedzić cyberprzestępców, którzy chcieliby zrobić z nich użytek. Jak widać na przykładzie linii produktów Kingston IronKey™ z funkcją szyfrowania sprzętowego, w ciągu wielu lat ich rozwoju opracowano i wprowadzono m.in. takie funkcje, jak 256-bitowe szyfrowanie AES w najsilniejszym trybie XTS, wytrzymała i odporna na fizyczną ingerencję obudowa, oprogramowanie sprzętowe z podpisem cyfrowym, klawiatury wirtualne oraz tryby hasła złożonego i wyrażenia hasłowego, aby ich użytkownicy byli naprawdę skutecznie chronieni przed wszelkiego rodzaju atakami.

Ponieważ świadomość cyberzagrożeń jest często bardzo mała, wiele firm zdecyduje się na korzystanie ze standardowych urządzeń pamięci mimo różnych luk w ich zabezpieczeniach. Pewną rolę odgrywa w tym ich łatwa dostępność, niski koszt i możliwość stosowania szyfrowania programowego, a także brak korporacyjnego procesu zatwierdzania pamięci flash. Zbyt często brakuje organizacyjnych zasad dotyczących najlepszych praktyk lub procesów zapewniających zgodność z różnymi standardami IT i wymogami w zakresie cyberbezpieczeństwa, takimi jak ISO27001, RODO, SOC2 czy najlepsze rządowe praktyki WISP. Oznacza to, że zagrożenia są często oceniane na podstawie opinii, a nie faktów, co sprawia, że wiele organizacji jest tak podatne na ataki.

Chociaż niektórzy korzystają ze standardowych urządzeń pamięci w połączeniu z dostępnymi narzędziami do szyfrowania programowego, często jest to złudna oszczędność, ponieważ wiele z nich może zostać zhakowanych przy użyciu bezpłatnych lub płatnych narzędzi dostępnych w Internecie. Funkcję szyfrowania programowego można również łatwo usunąć z urządzenia pamięci (dla wygody lub w celu korzystania na urządzeniach z nieobsługiwanymi systemami operacyjnymi) poprzez jego sformatowanie. Tymczasem urządzenia pamięci USB z szyfrowaniem sprzętowym mają zawsze włączoną funkcję szyfrowania, której nie można wyłączyć. Są one także skonstruowane w taki sposób, aby były odporne na próby fizycznej ingerencji, uwidaczniały ją i wykorzystywały cyfrowo podpisane oprogramowanie sprzętowe w celu zapewnienia autentyczności i integralności urządzenia. Ograniczenie liczby prób wprowadzenia hasła (ochrona przed atakiem metodą Brute Force) i wirtualne klawiatury (ochrona przed keyloggerami i screenloggerami) to kolejne dwie cechy szyfrowanych urządzeń pamięci takich jak IronKey VP50, zgodne z najlepszymi branżowymi praktykami walki z cyberprzestępcami, których celem jest wydobycie haseł od niczego niepodejrzewających użytkowników.



> Jeśli pamięć IronKey wykryje, że doszło do naruszenia oprogramowania sprzętowego, blokuje się i nie uruchamia, zwiększając w ten sposób cyberbezpieczeństwo. - Pasi Siukonen

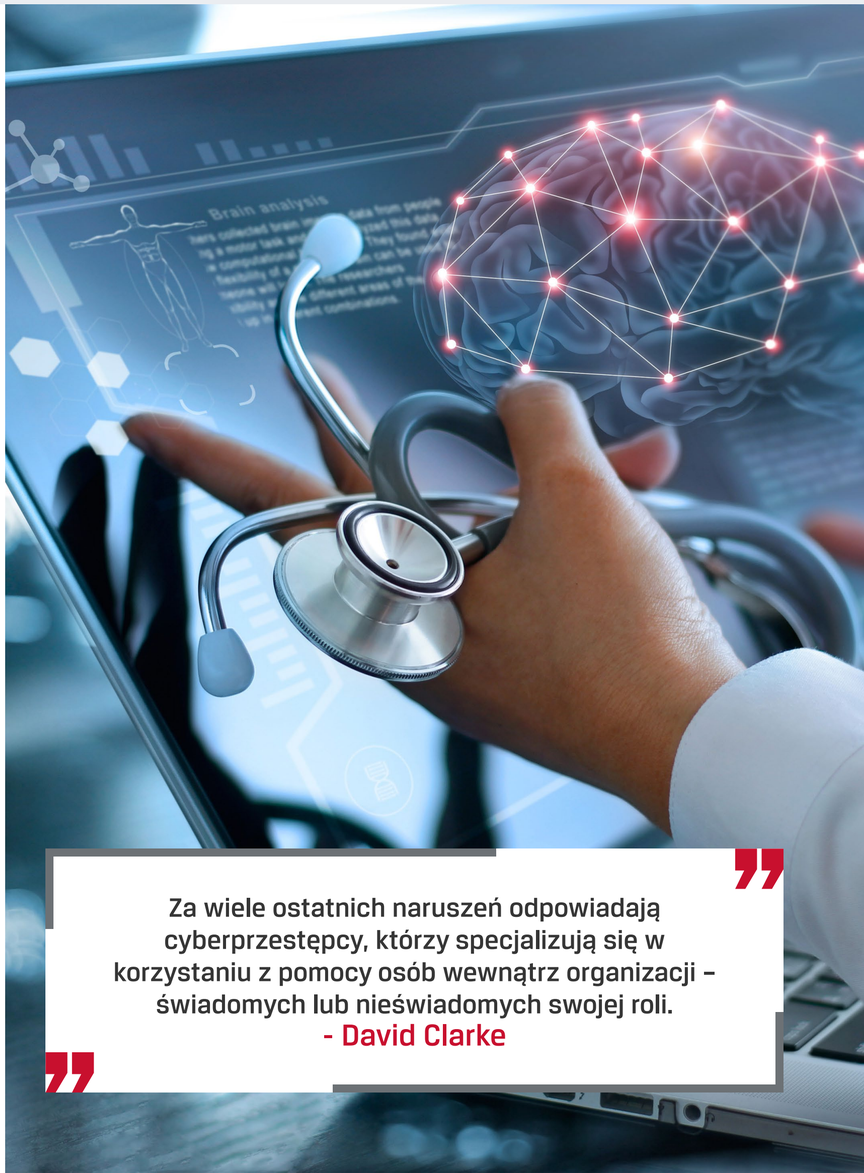
Kto jest zagrożony?

W rzeczywistości zagrożona jest każda firma, która nie jest w stanie kontrolować dostępu pracowników do urządzeń pamięci USB. W dodatku często nie jest świadoma, jakie dokładnie są to zagrożenia. Istnieją jednak czynniki, które mogą sprawić, że niektóre firmy będą bardziej atrakcyjnymi (i podatnymi) celami dla cyberataków.

Dane należące do firm z sektorów opieki zdrowotnej i finansów są nie tylko dużo bardziej atrakcyjne dla cyberprzestępców – ich naruszenie ma także znacznie bardziej dotkliwe skutki dla organizacji i ich klientów. Cyberatak wymierzony w 2017 r. w brytyjski NHS spowodował anulowanie ponad 19 000 wizyt i kosztował instytucję 92 miliony funtów z tytułu utraconych danych wyjściowych, a także kosztów przywrócenia danych i systemów. Nie tylko uniemożliwiło to pacjentom skorzystanie z opieki zdrowotnej, ale także sprowadziło na NHS dużą krytykę za to, że instytucja nie zareagowała wystarczająco szybko i skutecznie na wcześniejsze ostrzeżenia o zagrożeniach cybernetycznych. Podczas gdy wszystkie organizacje powinny być na bieżąco i dobrze poinformowane o cyberzagrożeniach, te, które mają do czynienia z informacjami wrażliwymi – w szczególności z danymi specjalnej kategorii – powinny zachować zdwojoną czujność.

Im wyższa jest wartość firmy mierzona obrotem, tym większych korzyści spodziewają się cyberprzestępcy i tym większe jest ryzyko ataku. Nie oznacza to jednak, że mniejsze organizacje nie powinny przejmować się cyberbezpieczeństwem. Choć duże przedsiębiorstwa mogą być bardziej atrakcyjnym celem ataków, często dysponują także odpowiednimi zasobami i specjalistami, aby móc stawić czoła zagrożeniom. Z drugiej strony wiele małych i średnich firm nie ma dedykowanych zespołów ds. cyberbezpieczeństwa i robi wyjątki dla kadry kierowniczej wyższego szczebla, aby uniknąć konieczności zarządzania urządzeniami pamięci USB, co sprawia, że są szczególnie narażone na niszczące skutki cyberataków. Niektóre badania pokazują, że małe i średnie firmy są w rzeczywistości częściej ich celem.

Ryzyko jeszcze większe w przypadku pracowników na wyższych stanowiskach kierowniczych. Są oni łatwi do wyśledzenia i często korzystają z przywilejów kierowniczych w swoich organizacjach, co oznacza, że nie stosuje się wobec nich procedur kontrolnych – także związanych z zarządzaniem urządzeniami pamięci USB. W efekcie są one wymarzonym celem dla cyberprzestępców. W tej sytuacji urządzenia z zawsze aktywnym szyfrowaniem sprzętowym, w połączeniu z odpowiednią wiedzą na temat cyberbezpieczeństwa i stosowaniem najlepszych praktyk i procesów, mogą w znaczącym stopniu zmniejszyć ryzyko i zapewnić ochronę przed atakami.



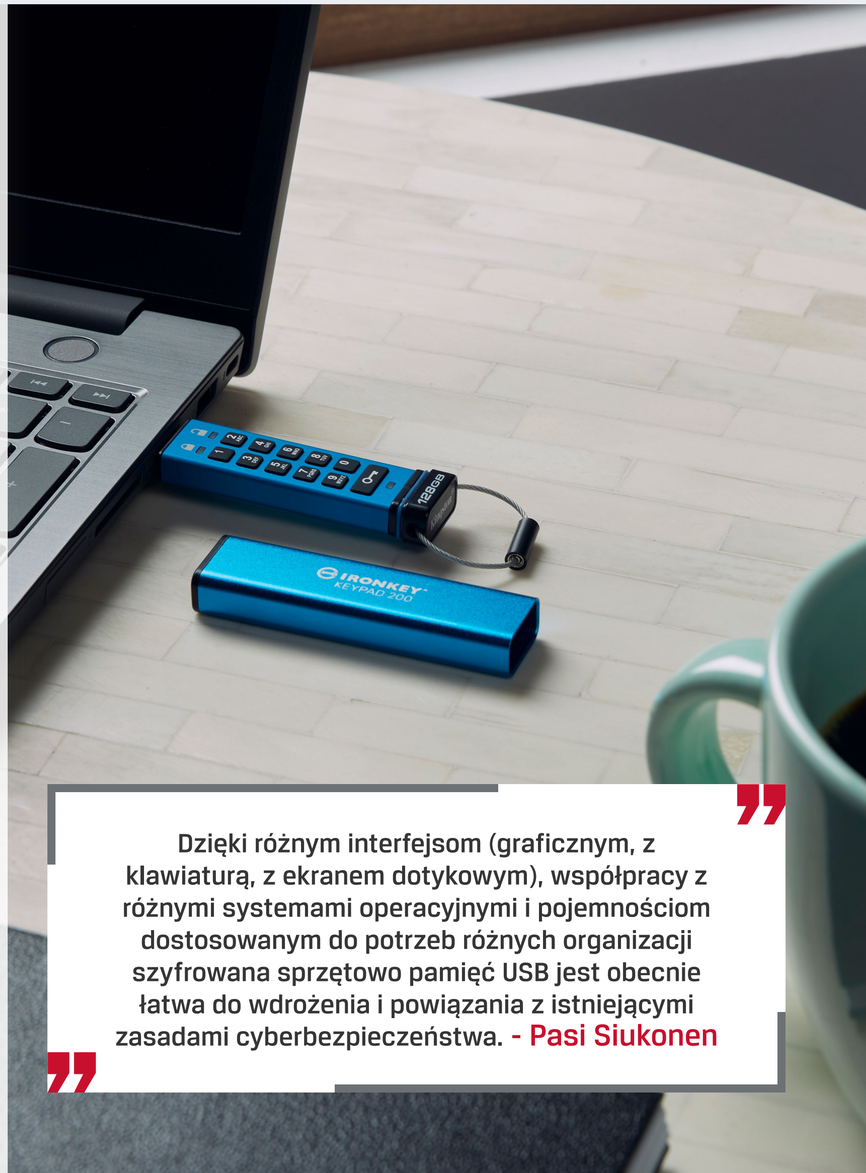
> Za wiele ostatnich naruszeń odpowiadają cyberprzestępcy, którzy specjalizują się w korzystaniu z pomocy osób wewnątrz organizacji – świadomych lub nieświadomych swojej roli.
> - David Clarke

Kto jest zagrożony?

> **Organizacje nie robią wystarczająco dużo, aby przeciwdziałać zagrożeniom dla cyberbezpieczeństwa.**
> **- David Clarke**

Kolejnym potencjalnym obszarem podatności organizacji na ataki jest łańcuch dostaw (ataki w tym obszarze są aż nazbyt częste). W 2013 r. amerykańska firma Target padła ofiarą jednego z największych naruszeń danych w historii branży handlu detalicznego, które skutkowało ujawnieniem informacji o kartach debetowych i kredytowych ponad 40 milionów klientów. Chociaż sama firma Target bardzo dbała o bezpieczeństwo cybernetyczne, czego dowodem było wdrożenie rozbudowanego systemu zabezpieczeń na 6 miesięcy przed atakiem, napastnicy przeniknęli do jednego z zewnętrznych dostawców firmy i w ten sposób uzyskali dostęp do jej głównej sieci danych. W sumie przeciwko firmie złożono 90 pozwów i straciła ona 61 milionów dolarów. Mimo, że sama nie była bezpośrednio odpowiedzialna za atak, to słabość zabezpieczeń w jej łańcuchu dostaw wystarczyła, aby spowodować szkody – zarówno finansowe, jak i wizerunkowe.

Źródłem podatności na ataki może być także obchodzenie zabezpieczeń przez pracowników. Chociaż może ono wynikać z chęci przyspieszenia codziennej pracy, zbyt często ignorowane są podstawowe zasady bezpieczeństwa i najlepsze praktyki, np. dotyczące zarządzania hasłami. Chociaż wytyczne NCSC i CISA są dosyć proste, często są one trudniejsze do wdrożenia w praktyce, zwłaszcza w przypadku osób, które są laikami w dziedzinie IT i cyberbezpieczeństwa. Chociaż z pewnością pomocne jest posiadanie zespołu ds. cyberbezpieczeństwa, już samo zapewnienie pracownikom odpowiednich narzędzi – takich jak urządzenia pamięci z funkcją szyfrowania sprzętowego – może znacznie zmniejszyć ryzyko wynikające obchodzenia zabezpieczeń.



> **Dzięki różnym interfejsom (graficznym, z klawiaturą, z ekranem dotykowym), współpracy z różnymi systemami operacyjnymi i pojemnościom dostosowanym do potrzeb różnych organizacji szyfrowana sprzętowo pamięć USB jest obecnie łatwa do wdrożenia i powiązania z istniejącymi zasadami cyberbezpieczeństwa. - Pasi Siukonen**

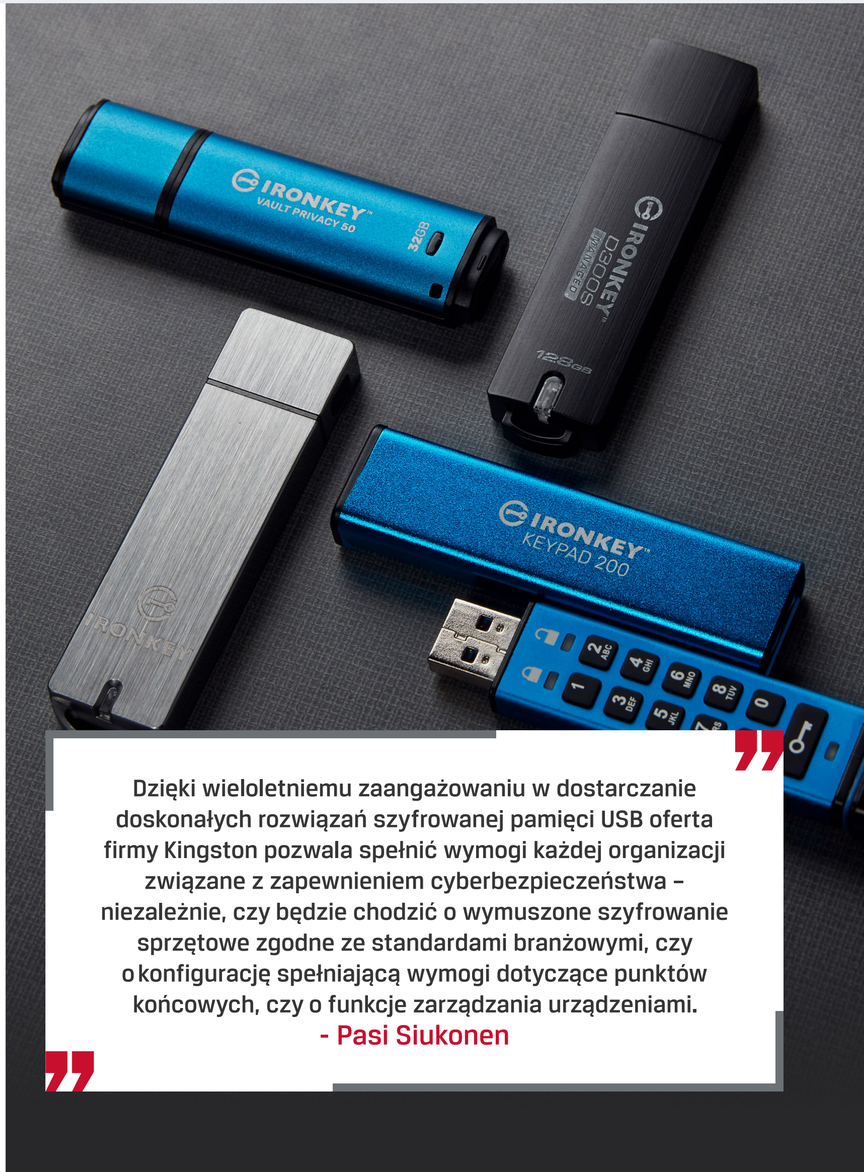
Jak organizacje mogą zmniejszyć ryzyko cyberataków?

Z organizacyjnego punktu widzenia można zrobić wiele, aby zabezpieczyć punkty końcowe i chronić dane. Bez zastosowania podejścia GRC (Governance – zarządzanie, Risk management – zarządzanie ryzykiem, Compliance – zgodność z przepisami) wszelkie dążenia do zapewnienia cyberbezpieczeństwa są skazane na niepowodzenie. Dlatego znajomość i przestrzeganie procedur jest niezwykle ważnym aspektem ochrony firmy. Posiadanie dobrego oprogramowania zabezpieczającego punkty końcowe może także zneutralizować wiele cyberzagrożeń – podobnie jak szybkie reagowanie i eliminowanie wszelkich dostrzeżonych luk w zabezpieczeniach.

> **To, czy przyjąć zasadę wymuszonego szyfrowania, czy nie, jest równie ważne, a być może nawet bardziej istotne dla zarządzania ryzykiem niż to, czy zdecydujemy się wykonać kopię zapasową danych.**
> - Pasi Siukonen

Jednak na poziomie jednostkowym szyfrowanie sprzętowe może radykalnie zmniejszyć podatność na zagrożenia dla cyberbezpieczeństwa. W obliczu wzrostu znaczenia i trwałości modelu pracy zdalnej i hybrydowej, zwłaszcza w połączeniu ze wzrostem liczby cyberataków w minionym roku, zapewnienie możliwości bezpiecznego przetwarzania, przesyłania i odczytu firmowych danych przez pracowników na każdym poziomie organizacji staje się ważniejsze niż kiedykolwiek dotąd. Urządzenia pamięci USB z funkcją szyfrowania sprzętowego pozwalają użytkownikom czerpać korzyści z przenośności i prostoty pamięci flash, jednocześnie znacznie zmniejszając ryzyko związane z jej użytkowaniem. Podczas gdy zgubienie lub kradzież standardowej pamięci może oznaczać utratę danych, pieniędzy i reputacji, pamięć szyfrowana sprzętowo została stworzona z myślą o ochronie poufnych danych przed wieloma zagrożeniami. A ponieważ cyberprzestępcy wciąż opracowują nowe sposoby ataków, szyfrowane urządzenia pamięci będą nadal ewoluować, aby sprostać tym wyzwaniom.

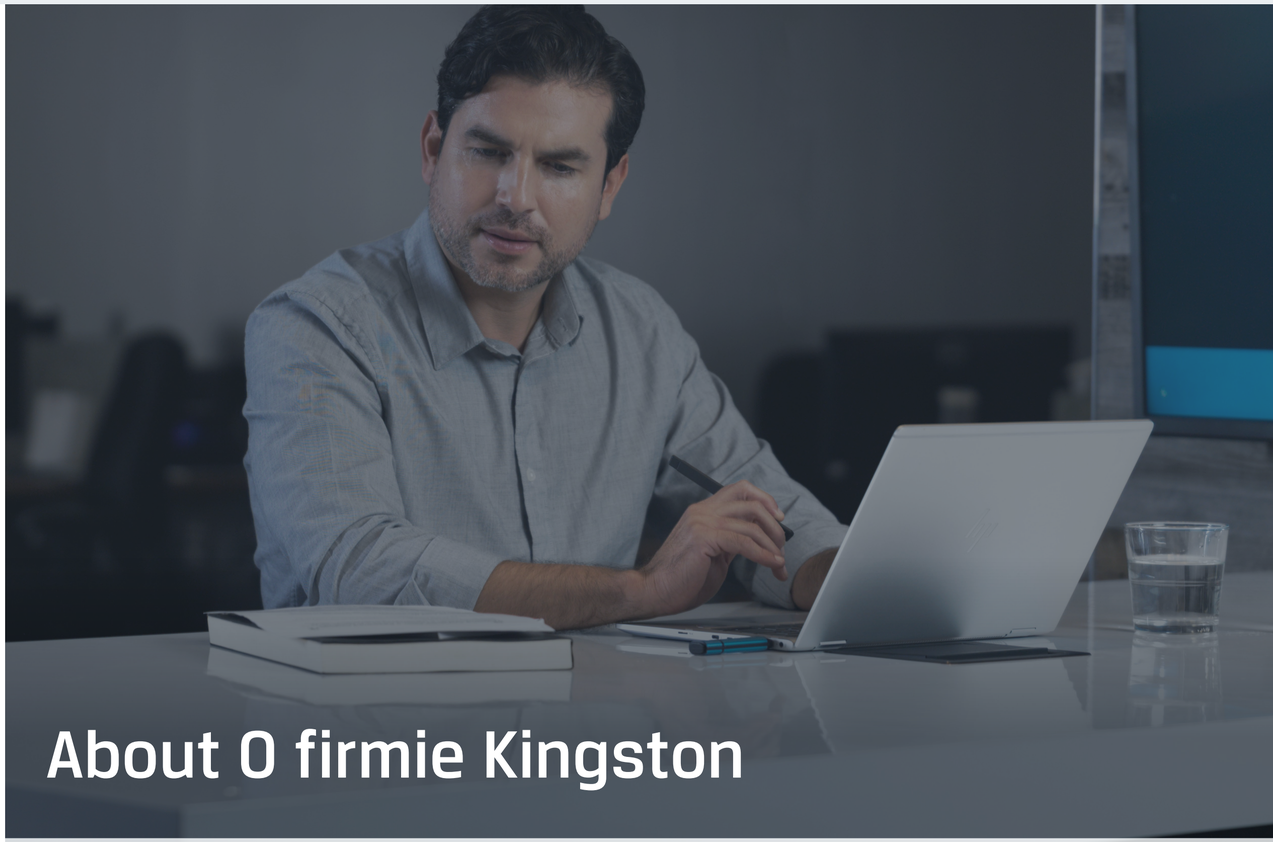
Ogólnie rzecz biorąc, koszty poniesione w następstwie cyberataku mogą być ogromne. Dlatego choć wprowadzenie i używanie szyfrowanej pamięci na poziomie organizacyjnym może wymagać bardziej wymagających procedur zatwierdzania i konfiguracji,na dłuższą metę może zaoszczędzić firmie dużo pieniędzy – zarówno jeśli chodzi o koszty związane z wymuszeniem, jak i o utratę przychodów z powodu nadszarpniętej reputacji. Same koszty obsługi prawnej związanej z naruszeniem danych mogą łatwo dorównać kosztom zakupu pamięci USB szyfrowanej sprzętowo.



> **Dzięki wieloletniemu zaangażowaniu w dostarczanie doskonałych rozwiązań szyfrowanej pamięci USB oferta firmy Kingston pozwala spełnić wymogi każdej organizacji związane z zapewnieniem cyberbezpieczeństwa – niezależnie, czy będzie chodzić o wymuszone szyfrowanie sprzętowe zgodne ze standardami branżowymi, czy o konfigurację spełniającą wymogi dotyczące punktów końcowych, czy o funkcje zarządzania urządzeniami.**
> - Pasi Siukonen

Podsumowanie

W firmie Kingston na bieżąco przyglądamy się rozwojowi sytuacji w obszarze cyberbezpieczeństwa i dbamy o to, aby nasze szyfrowane urządzenia pamięci IronKey były zgodne z najnowszymi wymogami i spełniały potrzeby w zakresie cyberbezpieczeństwa zarówno dużych, jak i małych organizacji. Ponieważ cyberbezpieczeństwo jest coraz większym problemem na całym świecie, jesteśmy przekonani, że dysponując odpowiednimi narzędziami i wiedzą, organizacje mogą być dobrze przygotowane do sprostania temu wyzwaniu, jednocześnie chroniąc siebie, swoich pracowników i klientów.



About O firmie Kingston

Dzięki ponad 35-letniemu doświadczeniu Kingston dysponuje wiedzą pozwalającą na identyfikację i rozwiązywanie problemów związanych z danymi mobilnymi, aby ułatwić pracownikom bezpieczną pracę bez narażania firmy.

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021