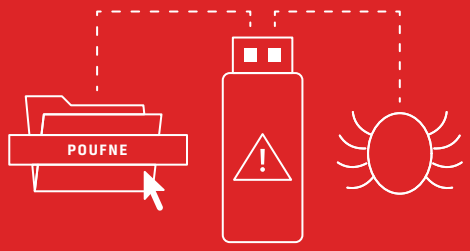
Uwaga na pamięci USB – jak zabezpieczyć dane?



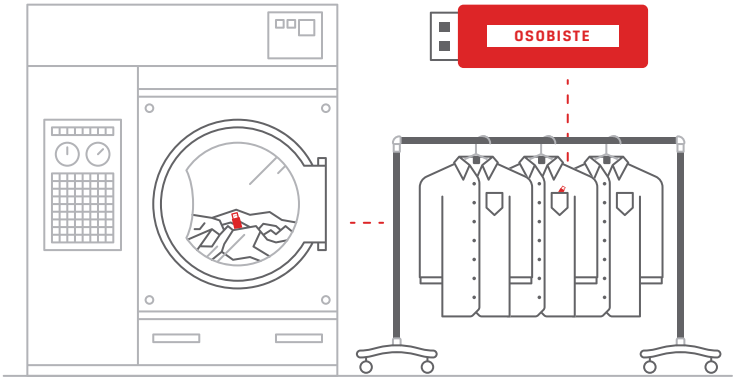
Pamięci USB zrewolucjonizowały sposób przenoszenia danych, jednocześnie powstały jednak nieznane wcześniej zagrożenia. Pamięci USB są powszechnie używane ze względu na łatwość ich przenoszenia i poręczność. Ale te właśnie cechy są też źródłem zagrożeń dla przechowywanych na nich danych. Jak można wyeliminować takie zagrożenia bez konieczności rezygnacji z wygody użytkowania pamięci USB?

Jakie są największe zagrożenia?

Pamięci USB są narażone na wielorakie ryzyko:

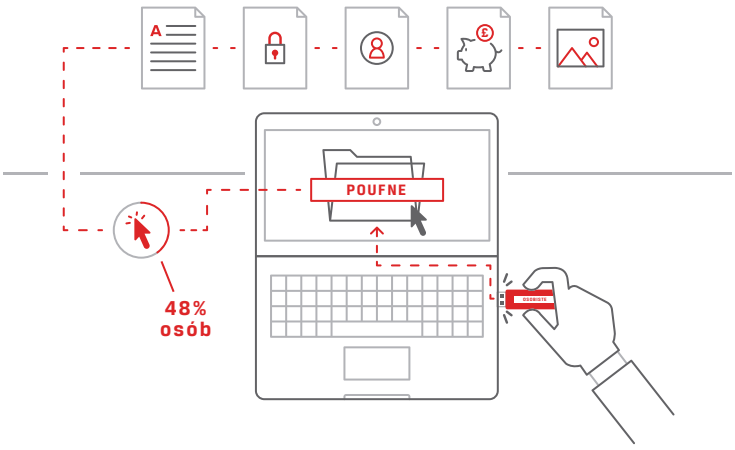
ZGUBIENIE

Do pralni trafia ponad **22.000 pamięci USB** rocznie[1]



ODNALEZIENIE

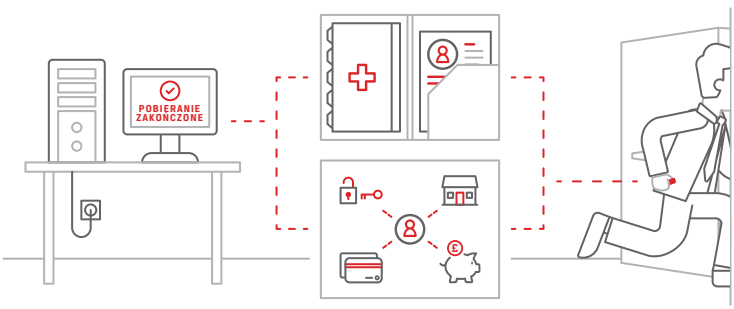
48% znalazców pamięci USB podłącza je i klika co najmniej jeden plik[4]



KRADZIEŻ

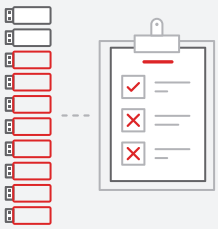
Z izby przyjęć szpitala ukradziono pamięć USB z poufnymi danymi **pacjentów**[2]

Niezadowolony pracownik wyniósł w pamięci USB dane **ok. 30.000 klientów banku**[3]



Jak profesjonalnie zabezpieczyć pamięci USB?

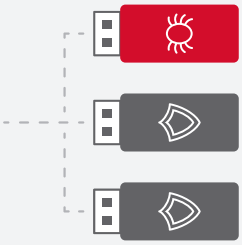
Przeprowadzone przez Spiceworks badanie wśród specjalistów IT pokazało, że większość organizacji zdaje sobie sprawę z ryzyka związanego z pamięciami USB, jednak niewiele z nich je wyeliminowało[5].



80% organizacji posiada polityki użytkowania pamięci USB

Najczęstszy sposób postępowania: ograniczenie uprawnień do użytkowania pamięci USB do określonych pracowników lub działów

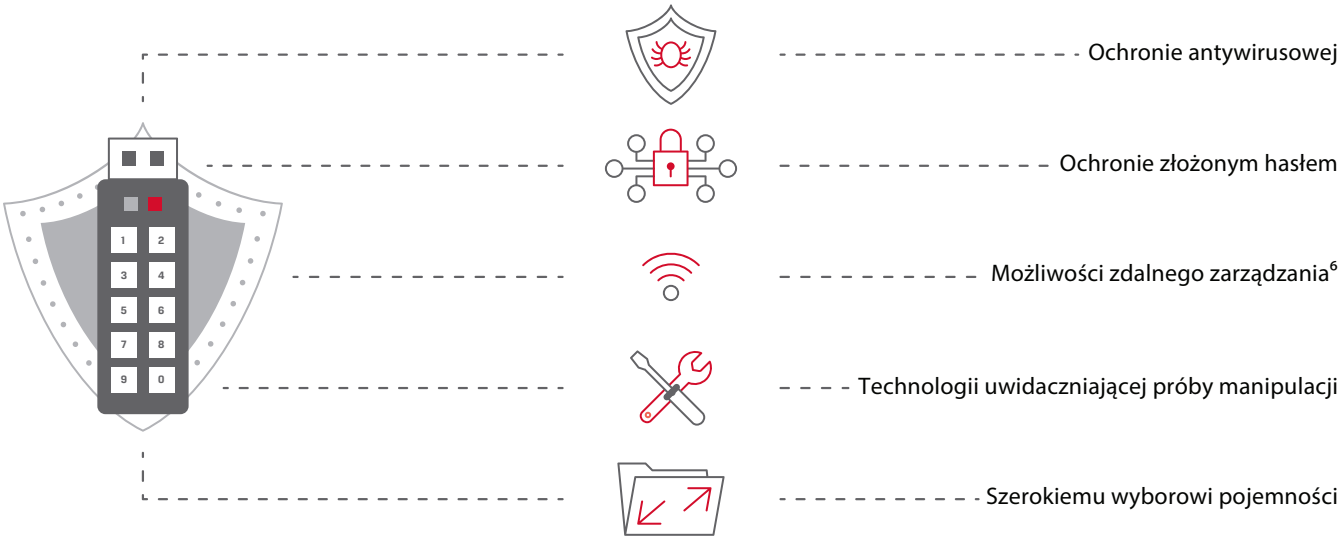
< 20% organizacji z takimi politykami wymaga używania szyfrowanych pamięci USB



Mimo to w ciągu ostatniego roku **1/3** badanych doświadczyła zagrożenia lub naruszenia bezpieczeństwa związanego z pamięciami USB

Szyfrowane pamięci USB nigdy nie zdradzają przechowywanych tajemnic

Szyfrowane pamięci USB gwarantują bezpieczeństwo i zgodność z przepisami, pozwalając skutecznie zamknąć tę często występującą lukę w zabezpieczeniach dzięki:



Zabezpiecz się dzięki produktom firmy Kingston

Oferowane przez firmę Kingston szyfrowane pamięci USB IronKey zapewniają ochronę najbardziej nawet poufnych informacji dzięki zgodności z najbardziej restrykcyjnymi regulacjami i protokołami bezpieczeństwa obowiązującymi agencje rządowe, usługodawców medycznych i instytucje finansowe.

Źródła:
1. Steve Bush, „22,000 USB sticks go to the dry cleaners", ElectronicsWeekly.com, 14 stycznia 2016. www.electronicsweekly.com/news/business/information-technology/22000-usbs-sticks-go-to-the-dry-cleaners-2016-01/
2. Taya Flores, „IU Health Arnett reports missing patient info", JConline, 5 stycznia 2016. www.jconline.com/story/news/2016/01/05/iu-health-arnett-reports-missing-patient-info/78300400/
3. Tom Brant, „Report: FDIC Employees Caused Repeated Security Breaches", PC Magazine, 15 lipca 2016. www.pcmag.com/news/346179/report-fdic-employees-caused-repeated-security-breaches
4. Elie Bursztein, „Concerns about USB security are real: 48% of people do plug-in USB drives found in parking lots", Elie.net, kwiecień 2016. www.elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots
5. Badanie Spiceworks wśród 300 decydentów IT w USA, Kanadzie i Europie na zlecenie firmy Kingston, luty 2017.
6. Firma Kingston Digital opracowała rozwiązania zarządzania szyfrowanymi pamięciami USB we współpracy z firmą DataLocker. www.kingston.com/us/usb/encrypted_security/management-solutions