Ryzyko ogólne oszacowano na poziomie: 3,99

ZALECENIA

Każdy przegląd infrastruktury IT powinien być udokumentowany w przyjęty w jednostce sposób.
Wyłączyć możliwość bootowania z innych niż dysk twardy nośników
Zablokować porty USB przed użyciem obcych nośników
Używać wyłącznie służbowe nośniki danych, które będą zabezpieczone szyfrowaniem
Prowadzić sprawdzenia logowania się użytkowników w korelacji z dniami wolnymi poszczególnych osób, aby wyeliminować wykorzystywanie wspólnie jednego konta przez większą ilość pracowników – przekazywanie innym osobom haseł dostępu
Zaszyfrować zawartości wszystkich nośników danych w sprzęcie, który może być wynoszony poza obszar przetwarzania, będzie to miało istotne znaczenie przy utracie sprzętu
Wskazane jest niezwłoczne wdrożenie polityki haseł narzuconych przez system operacyjny zgodnej z Polityką ochrony danych osobowych w zakresie częstotliwości ich zmiany.
Wskazane jest niezwłoczne wyeliminowanie z użycia sprzętu z systemem operacyjnym bez wsparcia producenta
Kopie zapasowe powinny być zabezpieczone kryptograficznie (szyfrowania) oraz fizycznie (przed ich utratą)
Przenieść pocztę elektroniczną na zasoby umożliwiające pełną kontrolę pod względem konfiguracji oraz odzyskania dostępu w przypadku przejęcia konta, a także z umową powierzenia, tworzącą kopie bezpieczeństwa, wolną od reklam i nadmiernej ilości spamu.
Dane osobowe pocztą elektroniczną należy przesyłać w zaszyfrowanych załącznikach.
Prowadzenie profili w mediach społecznościowych przez podmioty publiczne i przetwarzanie przez te profile danych osobowych jest wątpliwe pod względem istnienia podstaw prawnych takiego działania.
Zabezpieczyć linką kensington laptopy lub deponować je w szafach zamykanych na klucz po pracy