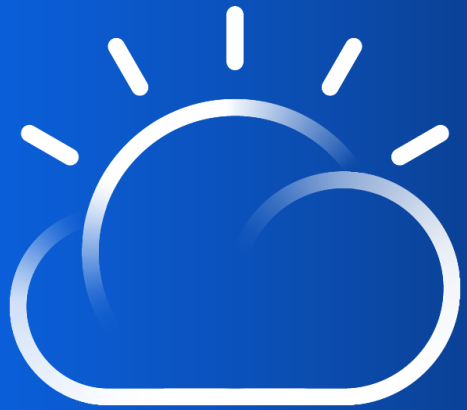
Jak bezpiecznie przetwarzać i przechowywać dane

nie tylko w trudnych czasach dzięki platformie IBM



Piotr Sękowski
Storage Sales Manager
IBM Poland & Baltics

IBM Cloud

Czy można przewidzieć przyszłość ?

Bill Gates ostrzegał w TED Talk 2015, że kolejnym wielkim zagrożeniem dla ludzkości był „wysoce zakaźny wirus”, na który „nie jesteśmy gotowi”.

https://www.ted.com/talks/bill_gates_the_next_outbreak_we_re_not_ready?language=pl

https://www.dailymail.co.uk/news/article-8132107/Bill-Gates-warned-2015-TED-Talk-big-threat-humanity-coronavirus-like-pandemic.html

Czy można przewidzieć przyszłość ?

“Jest rok 2022. Po oskarżeniach o prowokowanie niepokojów na świecie Rosja wypisuje się z organizacji międzynarodowych. Wojska Putina wkraczają na Ukrainę, by "utrzymać stabilność" w bratnim kraju, wywołując falę uchodźców, która szybko zalewa Europę”.

Serial “Years and Years“ (Rok z rokiem) z 2019

https://teleshow.wp.pl/trzy-lata-temu-serial-przewidzial-atak-putina-na-ukraine-przerazajaca-wizja-przyszlosci-6749647577635584a

Zmiana paradygmatu bezpieczeństwa

Które zagrożenie jest „niebezpieczniejsze”?

- Najbardziej prawdopodobne
- Najbardziej dotkliwe

Czy na pewno?

Wyzwania przyszłości wg Światowego Forum Ekonomicznego

- $4,62M w 2020
- $3.92M w 2019
- $3,86M w 2018
- Średni koszt wycieku danych w skali świata
  https://www.ibm.com/security/data-breach

$170.000

Średnia wartość okupu ataku

Źródło:
IBM security, 2021 Cost of Data Breach Study – https://www.ibm.com/security/data-breach
The State of Ransomware 2021 - https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

https://www.weforum.org/agenda/2020/01/top-global-risks-report-climate-change-cyberattacks-economic-political/

Czy ataki cybernetyczne dotyczą tylko innych ?

CyberDefence 24 ARMIA I SŁUŻBY POLITYKA I PRAWO SOCIAL MEDIA CYBERBEZPIECZEŃSTWO

Atak na Urząd Marszałkowski w Krakowie: nadal nie działa system informatyczny

24 CYBERDEFENCE24
15.02.2021 16:11

DRUKUJ PDF

fot. ali-a / pixabay

W tydzień od ataku hakerskiego nadal nie działa system informatyczny Urzędu Marszałkowskiego Województwa Małopolskiego. "Skupiamy się na przywróceniu funkcjonowania tego systemu, przy czym ważniejsze niż zrobienie tego szybko, jest by odbyło się to w bezpieczny sposób" - powiedział w poniedziałek PAP rzecznik marszałka województwa Dawid Gleń.

TVP3 ŁÓDŹ

Hakerski atak na Urząd Gminy w Lututowie

2019-12-19 | LUTUTÓW (POW. WIERUSZOWSKI) UDOSTĘPNIJ:

Wójt Lututowa nie ujawnia jak dużego okupu zażądali hakerzy/fot. TVP3 Łódź

Hakerzy żądając okupu zaszyfrowali dostęp do bazy danych programów księgowych i podatkowych instytucji. Tym samym mieszkańcy nie mogli uzyskać informacji o swoich opłatach czy zaległościach.

SERWIS SAMORZĄDOWY PAP

Prawo Finanse Edukacja Środowisko Praca E-urząd Komitet Regionów Klub Samorządowy PAP

E-urząd

Urząd miejski w Otwocku padł ofiarą cyberataku

Marcin Mastalerz 22.10.2021 Aktualizacja: 24.10.2021, 23:00

Zdjęcie ilustracyjne; Fot. PAP/EPA

System komputerowy otwockiego magistratu został zaatakowany przez hakerów, którzy zaszyfrowali dane znajdujące się na serwerach urzędu. W efekcie cyberataku obsługa mieszkańców w takich sprawach jak karty metropolitarne, karty dużej rodziny, karty 3+, załatwianie spraw podatkowych oraz gospodarki odpadami odbywa się z utrudnieniami.

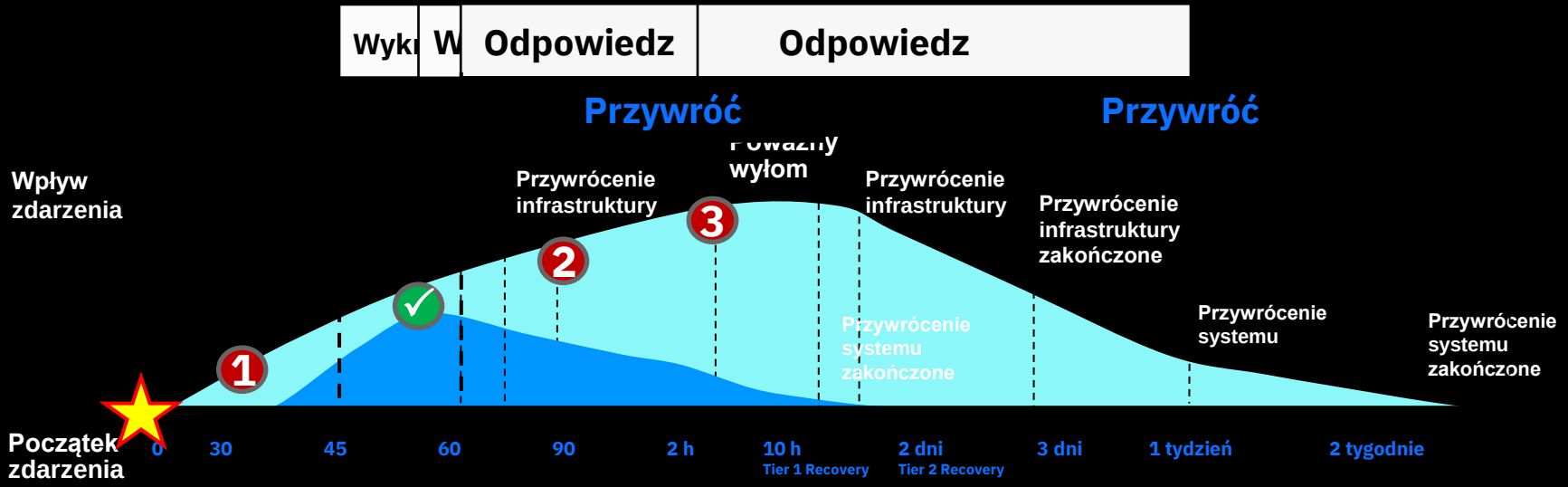
Najpopularniejsze

1. MEiN przedstawiło w nauczycieli specjalist szkolnym
2. Powstaje lista zagroż Inwestycji Strategicz
3. MF o ujmowaniu zak samorządach
4. Terlecki: ustawa o pr samorządowych już
5. Urzędnicy nie chcą d wyjazdów. Apel o wa

Jak się przygotować?

Detekcja i reakcja na atak

Atak w funkcji czasu

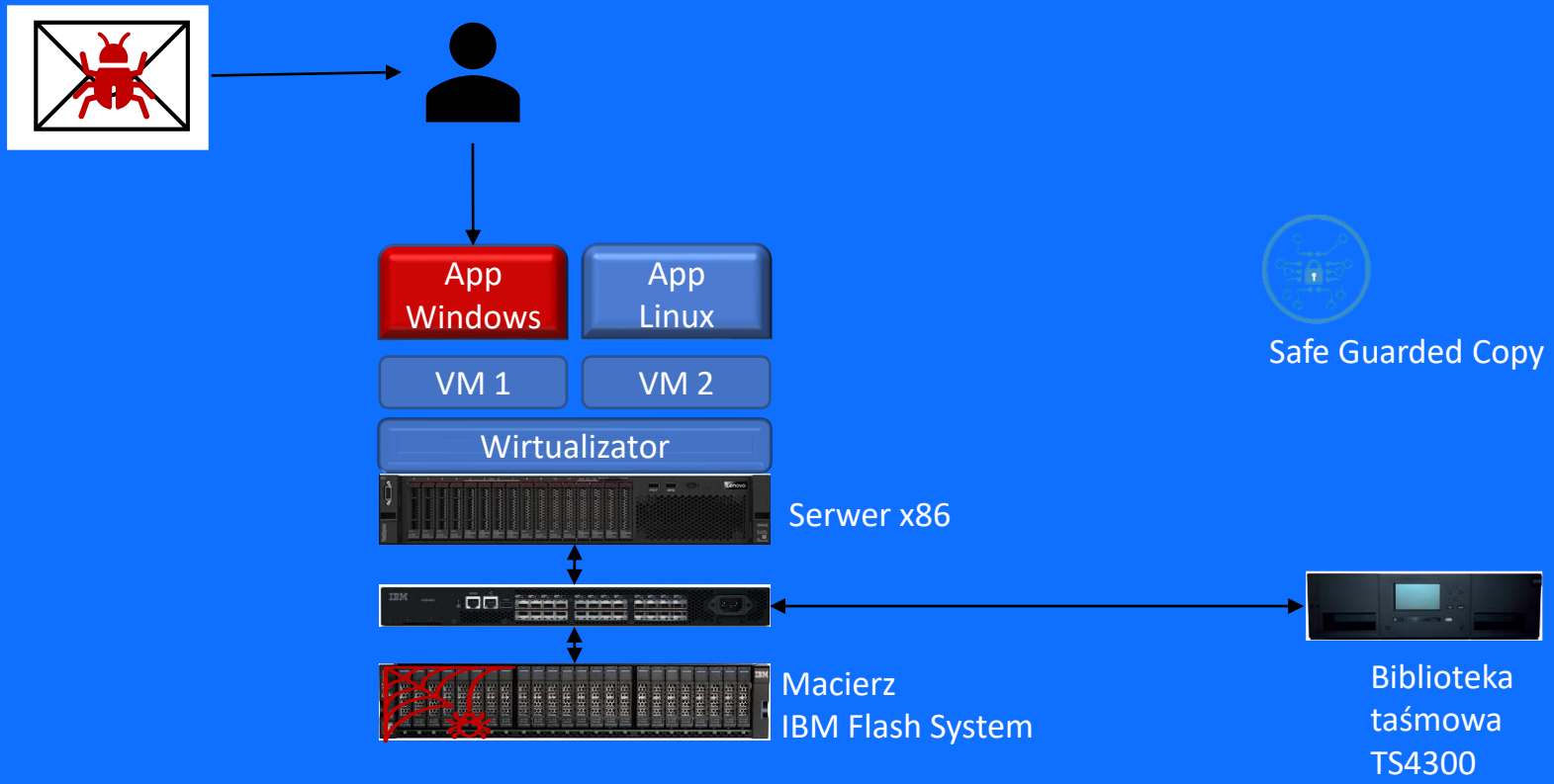


1. Dane ulegają uszkodzeniu – incident nie jest wykryty
2. Bez Cyber Vault uszkodzenia danych w środowisku są wykrywane dużo później i mają dużo większy wpływ na nasze działanie
3. Jeśli uszkodzone dane zostały zreplikowane lub wykorzystane przez inne systemy czas wymagany na identyfikację i mitygację uszkodzeń wydłuża się diametralnie

IBM Cyber Vault Effect

Dzięki środowisku Cyber Vault i zastosowaniu technologii Safeguarded Copy dane są stale sprawdzane, a uszkodzenia są wykrywane i naprawiane WCZEŚNIEJ I SZYBCIEJ

Przykładowy atak - co się w dzieje IT

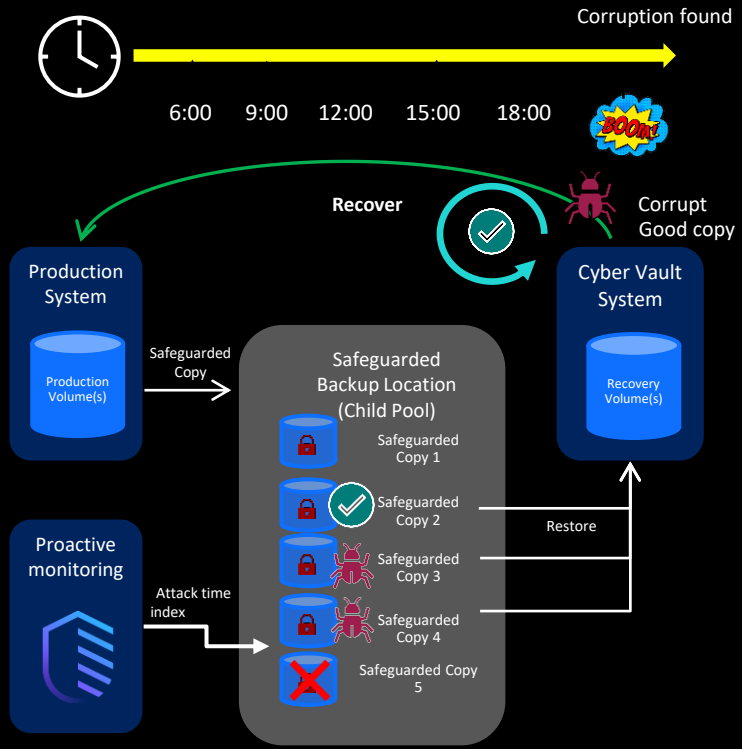


Safeguarded copy jak działa?


FlashSystem 9500


FlashSystem 7300


FlashSystem 5200



Safeguarded copy gdzie działa?


FlashSystem 9500


FlashSystem 7300


FlashSystem 5200

Macierz typu Dual Active-Active 1U
Full NVMe
12 dysków półce kontrolnej
rozbudowy o 20 półek 2U lub 8 półek 5U

Dyski – FlashCoreModule FCM 3.0

Ta sama sprawdzona technologia SLC/QLC

Od 4.8 do 38.4TB fizycznej pojemności

Sprzętowa kompresja 3:1

Pojemności do 22, 29, 58, 116TB

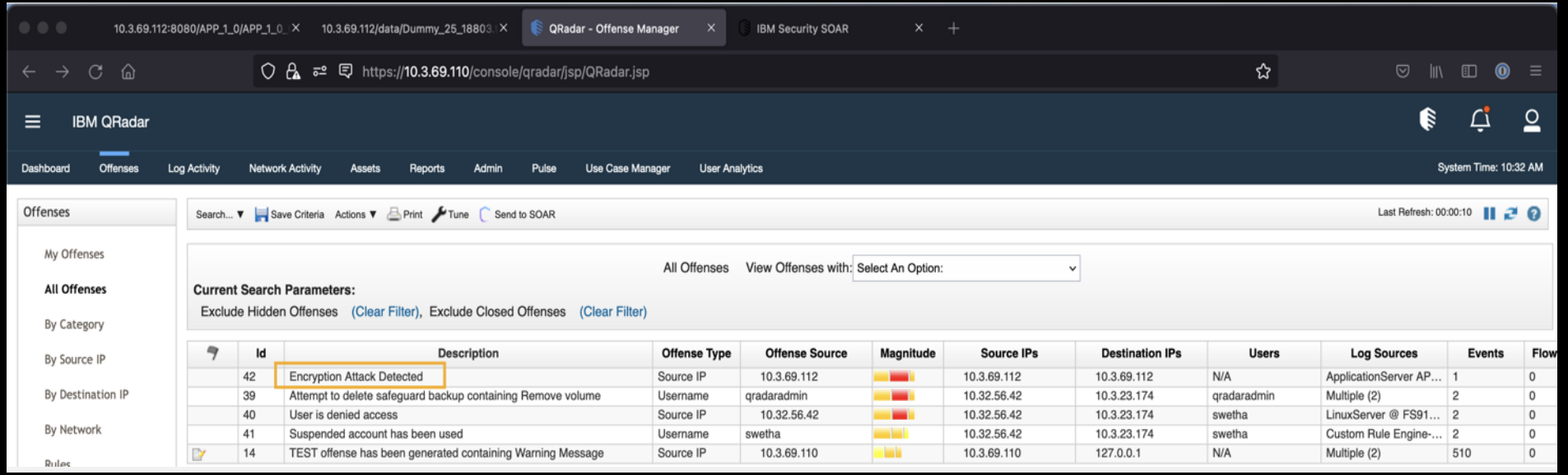
PCIe gen 4 w technologii 7nm dla modułów 19.2 i 38.4TB

Monitoring ruchu aplikacyjnego

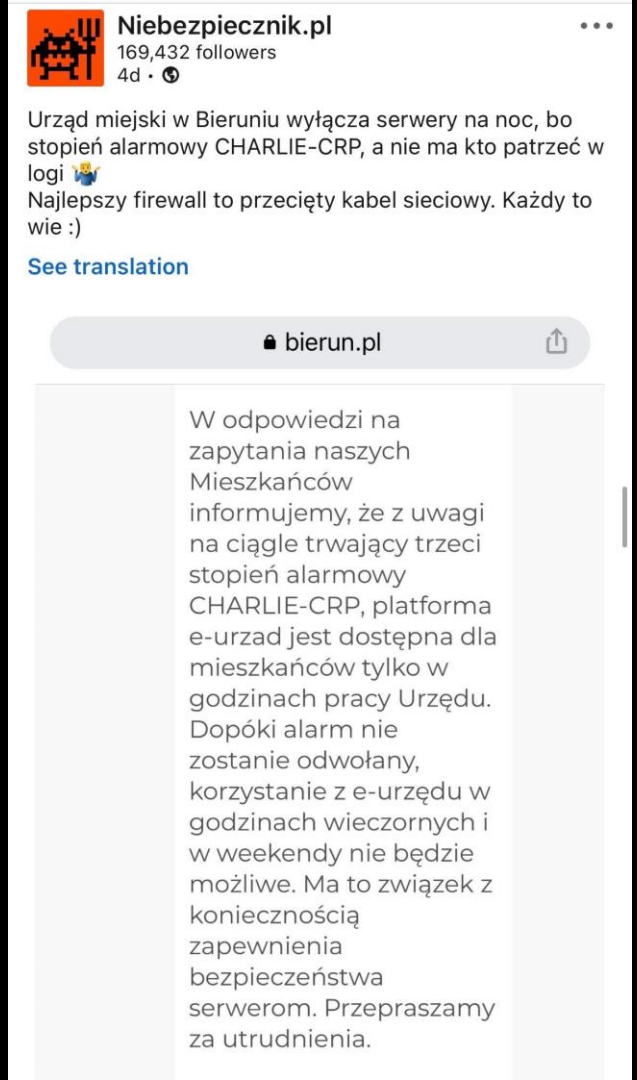
IBM QRADAR

Aplikacje krytyczne

Monitorowanie zasobów



~~Monitoring ruchu aplikacyjnego~~
Ręczne zarządzanie ruchem aplikacyjnym



Czy można przewidzieć przyszłość

Hackers abuse single bit change in Intel CPU register to evade detection

Palo Alto Networks discovers that Trap Flag is being abused to notify malware it is being analyzed

by: Rene Millman 20 Jul 2021

Shutterstock

Security researchers have discovered a specific single bit (Trap Flag) in the Intel CPU register that malware can abuse to evade sandbox detection.

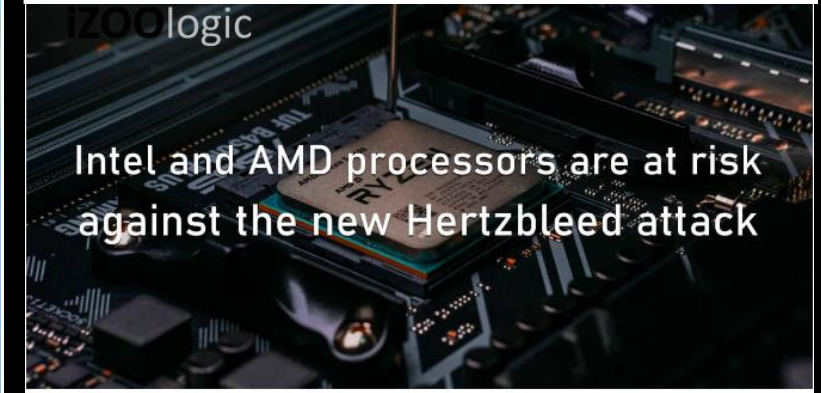
According to researchers at Palo Alto Networks' Unit 42 threat research group, malware can detect whether it is executing in a physical or virtual machine (VM) by monitoring the response of the CPU after setting this single bit.

https://www.itpro.com/security/malware/360299/hackers-use-single-bit-change-in-intel-cpu-register-to-evade-detection

Intel and AMD processors are at risk against the new Hertzbleed attack

June 17, 2022 By iZOOlogic

In Digital Risk Protection, Third Party Risk Assessment



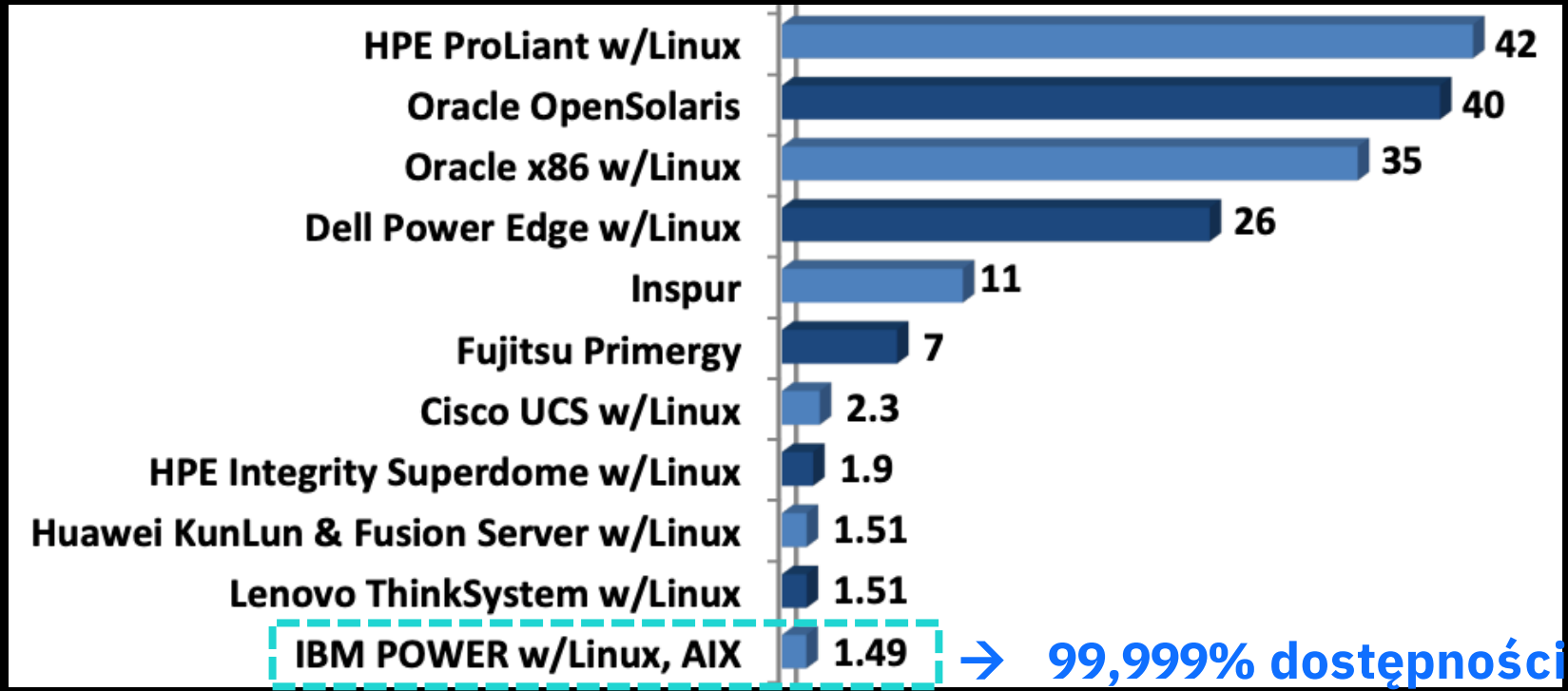
Remote threat operators can now execute a new side-channel attack tracked as Hertzbleed. They use the new attack vector to exfiltrate full cryptographic keys in affected CPUs through observing their frequency variations enabled by DVFS or dynamic voltage and frequency scaling.

According to the security analysts, the new side-channel attack is highly effective on modern Intel and AMD x86 processors since the DVFS is dependent on the power consumption and processed data. DVFS helps adjust a computer processor's power and speed settings, which is vital in reducing power consumption and optimising its efficiency.

https://izoologic.com/2022/06/17/intel-and-amd-processors-are-at-risk-against-the-new-hertzbleed-attack/

Niezawodność i bezpieczeństwo

Roczny czas nieplanowanego przestoju serwerów [min]

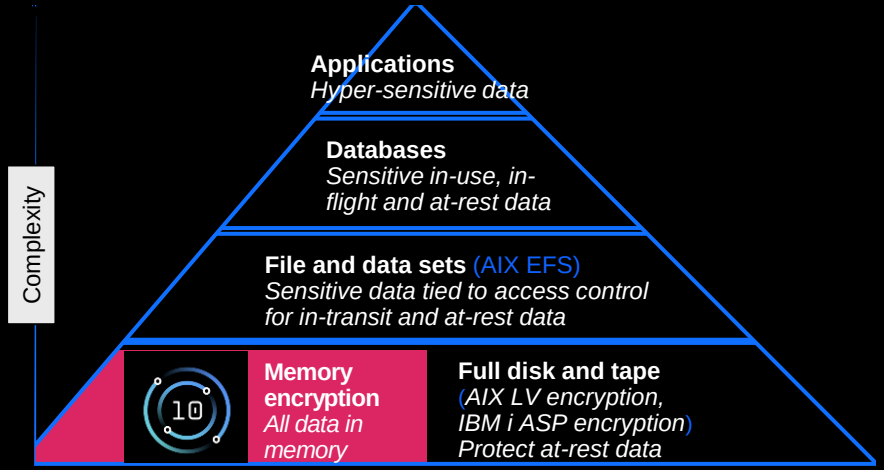


Źródło: https://www.lenovo.com/us/en/resources/data-center-solutions/analyst-reports/itic-2021-global-server-reliability-report/

Ochrona przetwarzania

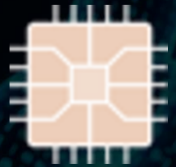
SERWERY IBM POWER 10

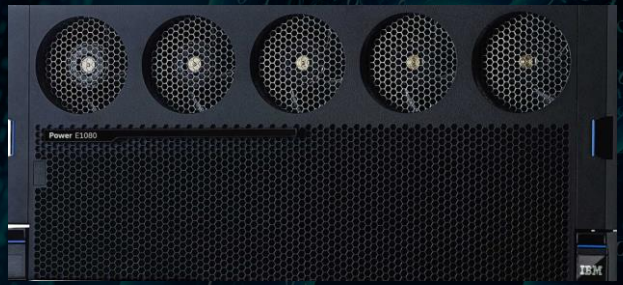
Chroń dane w pamięci za pomocą przezroczystego szyfrowania pamięci



Szybkie szyfrowanie z akceleracją sprzętową

- 4X silniki kryptograficzne w każdym rdzeniu





Wyprzedź obecne i przyszłe zagrożenia dzięki:

- Bezpieczna kryptografia kwantowa

Quiz

Jak nazywa się funkcjonalność storage dająca możliwość szybkiego odtworzenia po ataku ransomware?

IBM SAFE GUARDED COPY

Narzędzie do ciągłego monitoring bezpieczeństwa systemów IT?

IBM QRADAR

Który product jest gotowy na odparcie ataku komputera kwantowego?

SERWERY IBM POWER 10

IBM

www.linkedin.com/in/sekowskipiotr/