IBM Security

e-government 20:10

Jak čelit aktuálním hrozbám v roce 2022

IBM Security Services

Miloš Soukup – CEE Security Solution, EMEA Solution Design – Security Services

Září 2021

IBM

Přehled:

Celkové náklady rostou

10% nárůst

průměrné náklady spojené s únikem dat, se zvýšily o 10procent. To je nejvíce za posledních 7let

11 let

jsou zdravotnické organizace Ty, které jsou nejvíce postiženy zvýšenými náklady za ztrátu dat

Evropa, USA, Střední východ

rozšiřující se oblasti v kterých jsou detekovány ransomware a další útoky. Evropa byla nejvíce postižená lokalita kyber útoky

Jaké jsou hrozby

Nejčastější

23%

všech detekovaných útoků připadá na útoky Ransomware jen Evropě (ostatní 33%)

Typy útoků

35%

připadá na scan and exploit zranitelnosti, phishing až na druhém místě

Změna cílů

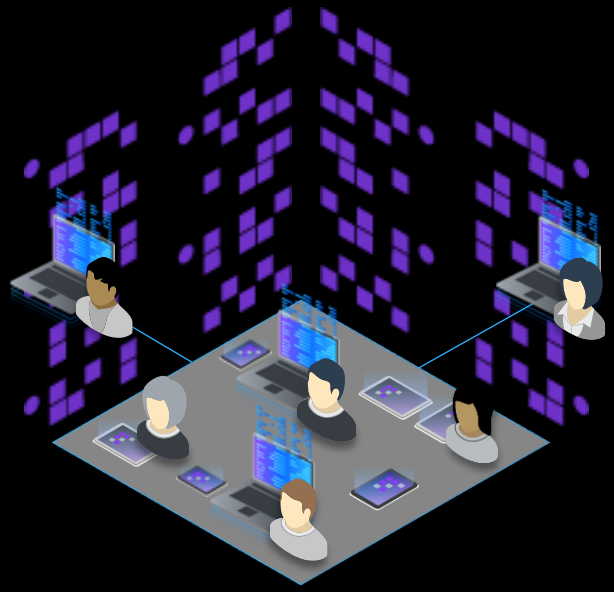
56

počet nových malware hrozeb detekovaných pro Linux systémy. Dramatický meziroční nárůst

[1] X-Force Threat Intelligence Index 2021
[2] Global Threat Landscape Report, August 2021
[3] X-Force Cost of Data Breach Report 2021

Styl práce se změnil a neustále se mění

Priority organizací jsou poháněny digitalizací (nejen) státní správy



Uživatelé a koncová zařízení

Přístup odkudkoliv a ideálně z jakéhokoliv prostředku (zařízení)

Aplikace a Data

Data jsou sdíleným zdrojem jak pro uživatele tak pro aplikace

Infrastruktura

Servery a sítě jsou rozkročené mezi onPremise řešením a Cloud prostorem (např. hybridní Cloud)

... výsledná složitost snižuje obranyschopnost zavedených modelů

Zero Trust framework jako pilíř pro strategický přístup (Google, Forrester, Gartner, NIST)

Nikdy nevěř, vždy oveřuj

Nasazuj nejnižší oprávnění

Očekávej cokoliv

Obchodní přístup při řešení bezpečnostních témat znamená použití zero trust principů pro top priority

Ochrana soukromí

Zjednodušte a zajistěte nástup a nastavení zaměstnanců. Spravujte uživatelské preference a souhlas Prosazujte a kontrolujte používání norem na ochranu osobních údajů

Interní útočník

Vynutcujte přístup s nejmenšími oprávněními. Zajistěte detekci rizikové chování uživatelů. Zajistěte dodatečné zdroje (Threat Intelligence)

Cloud

Spravujte a kontrolujte všechny přístupy. Monitorujte aktivitu a konfigurace cloudu.

Vzdálený přístup

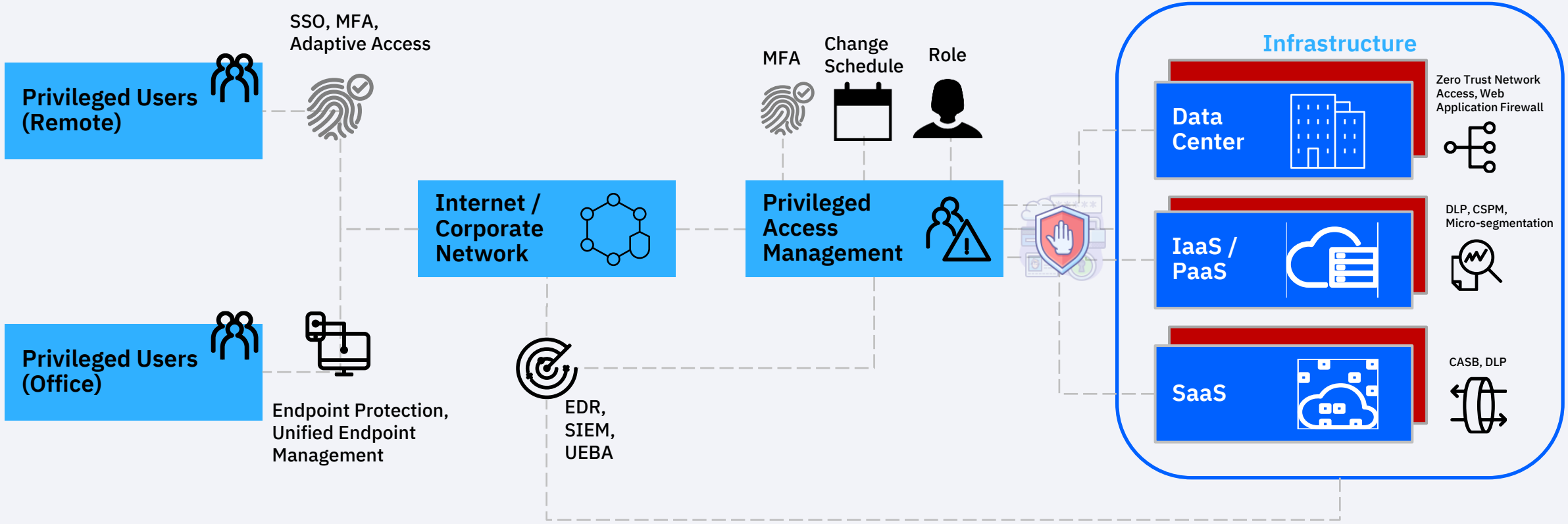
Zabezpečte BYOD a nespravovaná zařízení. Nastavte politiky. Odstraňte nepoužívané VPN. Poskytujte školení

“ZeroTrust nám pomáhá aktivovat důležité obchodní při správě zabezpečení”

- CISO, Global Chemical Manufacturer

Zero Trust – Ochrana privilegovaných uživatelů

Další Use Case: Ochrana před interním útočníkem, Ochrana vzdáleném přístupu do kanceláře



Zero Trust Maturity Level	1. Ad-Hoc	2. Repeatable	3. Defined	4. Managed	5. Optimized
	Mannuální vytváření účtů kopií ze stávajícího administrátora s manažerským oprávněním	Nasazení nástroje (PAM) pro kontrolu dané aplikace nebo dedikovaného prostředí.	Nasazení nástroje (PAM) napříč celou organizací, pro všechny privilegované účty (externí, interní, IT, Management)	Integrace s dalším i technologiemi pro MFA, Řízení oprávnění, SIEM/SOC, apod.	Začlenění algoritmu pro adaptivním rozhodování přístupu. Integrace s dalšími bezpečnostními technologiemi pro zajištění obohacení dat, automatizace zásad zabezpečení.

Doporučení:

- Rychlejší detekce a eliminace hrozby
- Zálohování
- Pravidelná kontrola konfigurací a patch management
- Trénink personálu
- Implementace MFA
- Ochrana před Insider-y (nejen DLP)
- Bezpečný vývoj
- Aktualizace plánů reakce, příprava a provádění stres testů

Definujte si požadavky pro použití Zero Trust use cases

Security Domain

Security Sub-Domain / Control

Security Domain					
Governance	Strategy	Policy Administration	Architecture and Design Stds.	Awareness & Education	Risk and Compliance
Data	Classification / Labeling	Data Services (WH, Lakes, DB)	Encryption	DLP / CASB	Threat Monitoring, Detection, and Response
Application	Enterprise App. Access	Cloud / As-a-Service Access	API Access	DevSecOps / Production Rel.	SOC
Identity and Access	Joiner, Mover, Leaver (JML)	Authentication / MFA / Az	Privileged Access	Identity/Access Governance	Security Testing
Infra & Endpoint	Platform Access	Device Access (inc. BYOD)	Edge Access	Cloud Service Access	Threat/ Vuln. Management
Network	NAC	VPN Access	Remote Virtual Desktop Access	Wi-Fi / LAN Access	Dashboard / Reporting
Physical	Perimeter Access	Building Access	Office Access	Secured Area Access	

Branch Offices (Dealerships) Security

Enterprise IT Security (Backoffice /DC)

Operational Technology (OT) Security

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity