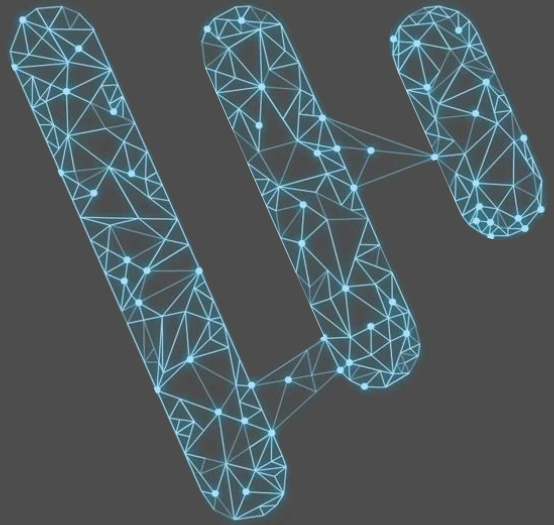



CRA
ČESKÉ RADIOKOMUNIKACE

JAK ZAJISTIT BEZPEČNOST V CLOUDOVÉM PROSTŘEDÍ

LUKÁŠ BARTAKOVIČ, MAREK ERNEKER

29. ČERVNA 2021

AGENDA:

- O čem bude dnešní webinář?
  - Trend bezpečnosti v cloudu
  - Metody obrany
  - Doporučení a další kroky
- Dotazy:
  - Do chatu
  - Offline
    - Telefon
    - email

PRINCIP CLOUDU

MOTIVÁTORY PRO CLOUD

Proč uživatelé volí stále častěji cloud

- Motivátory pro přechod do cloudu
  - Pružnost
  - Bez vysokých investic
  - Neřeší zastarávání HW a podporu
  - Požadavky na bezpečnost a legislativu
  - Digitální transformace
  - Snížení nákladů
  - Požadavky na zajištění dostupnosti

- Jak to pomůže zákazníkovi
  - Bezpečnost na úrovni kritické infrastruktury
  - Globální bezpečnostní standardy
  - Best-in-breed technologie
  - Konsolidace služeb a informací

Soustředíme se na to, v čem jsme dobří. A co nám vydělává peníze.

DNEŠNÍ DOBA A DIGITÁLNÍ TRANSFORMACE

CoVid akcelerátor změn

- CoVid-19 urychlil digitální transformaci
  - Z roků na měsíce
  - (*Zdroj: https://www.twilio.com/covid-19-digital-engagement-report*)
  - 95% společností mění způsob komunikace se zákazníkem
  - 92% společností soudí, že změna digitální komunikace je potřebná pro business

- Po odeznění pandemie
  - 92% společností chce rozšířit digitální komunikaci i po znovuotevření
  - 53% společností přidá nový způsob oslovení zákazníků jako důsledek pandemie
  - Světové společnosti (a stát) získali povolení (a odvahu) inovovat.
  - Zvýšení budgetů

PILÍŘE BEZPEČNOSTI V ONLINE SVĚTĚ

Základní členění bezpečnosti nejen v cloudovém světě

Detekce

- Flow monitoring
- Performance monitoring
- SIEM
- SOC
- Vulnerability management
- Account activity
- ML, AI

Incident response

- SIEM
- SOC
- EDR/XDR
- Automatizace

Správa uživatelů a přístupů

- Adresářové služby
- SSO
- PAM
- VPN

Ochrana infrastruktury

- DDoS Ochrana
- WAF
- Firewall
  - (next-gen)
- Mikrosegmentace
- VPN/ZTNA
- SASE

Ochrana dat

- Zálohování
- DR
- Ochrana před APT
- Sandboxing
- API Security

Compliance

- Audity
- Směrnice
- Bezpečnostní politiky

MATICE SDÍLENÉ ODPOVĚDNOSTI

Za co odpovídá zákazník a za co poskytovatel služby

	IaaS	PaaS	SaaS
Uživatelé	Zákazník	Zákazník	Zákazník
Data	Zákazník	Zákazník	Sdílená odpovědnost
Aplikace	Zákazník	Zákazník	Cloud provider
Operační systém	Zákazník	Sdílená odpovědnost	Cloud provider
Virtuální sítě	Sdílená odpovědnost	Cloud provider	Cloud provider
Virtualizace	Cloud provider	Cloud provider	Cloud provider
Servery a uložiště	Cloud provider	Cloud provider	Cloud provider
Fyzická infrastruktura	Cloud provider	Cloud provider	Cloud provider

ODPOVĚDNOST ZÁKAZNÍKA/UŽIVATELE

Výzvy se zajištěním bezpečnosti

Do roku 2025 bude 95-99% bezpečnostních incidentů v cloudu způsobeno chybou zákazníka *(Gartner)*

- *Nelze spoléhat na to, že co je v cloudu je automaticky bezpečné*

Odpovědnosti zákazníka

- Ochrana dat a obsahu
- Správa aplikací a uživatelů
- OS, Firewall, Network settings
- Šifrování a zabezpečení komunikace

Zákazník provozuje aplikace v cloudu

- Je Cloud bezpečný vs Používám Cloud bezpečně?
- Analýza rizik – jaká data do cloudu a za jakých podmínek

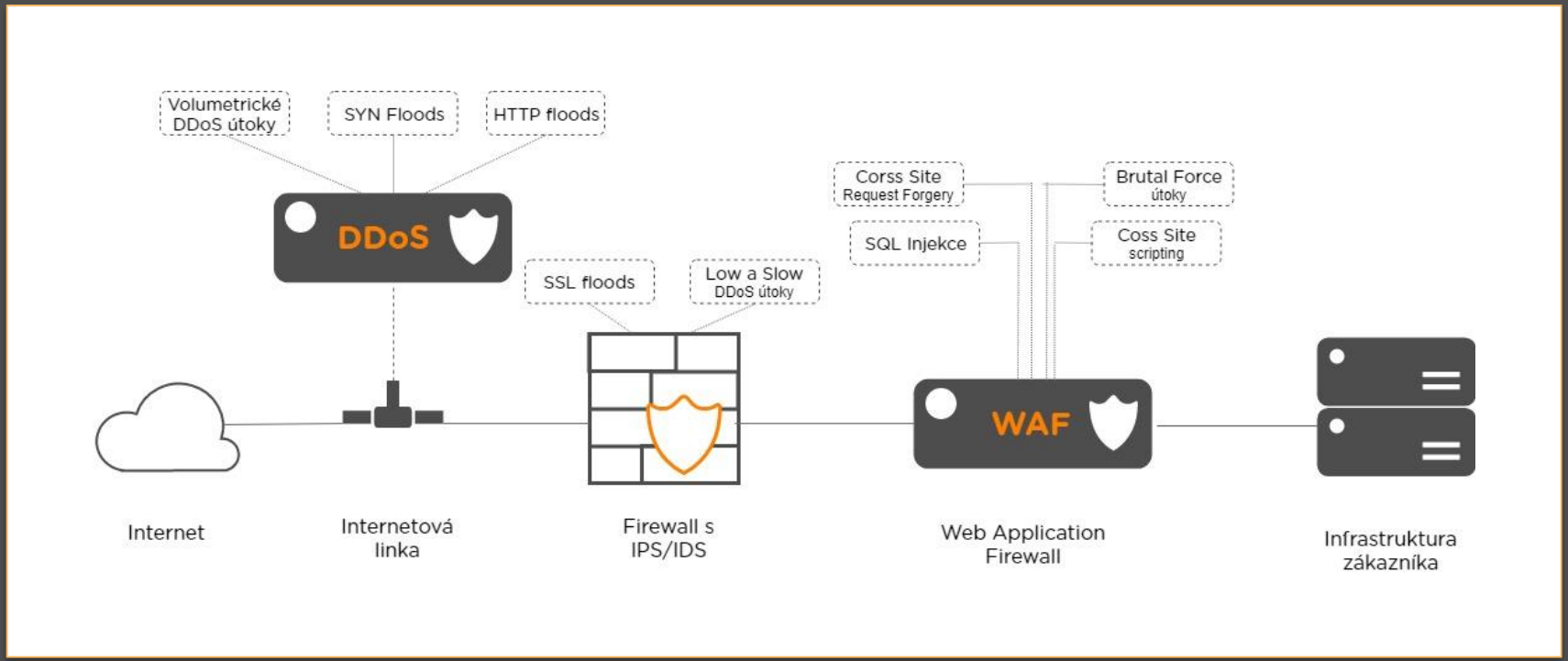
- Jak zajistím bezpečnost?
- Sám vs formou služby

OCHRANA INFRASTRUKTURY

Služeb a aplikací v cloudovém prostředí

OCHRANA INFRASTRUKTURY

Základní koncepce



OCHRANA SÍŤOVÉHO PERIMETRU

DDoS Ochrana

- DDoS útoky
- Cílem vyřadit, znepřístupnit cílové zařízení nebo službu
  - Služby citlivé na dostupnost
  - Výpadek znamená vysoké škody

- Nárůst počtu útoků o 515% YoY (2019/2020)
- 70% útoků kratších než 90 minut
- 90% pod 1 Gbps
- Útok více vektory
- Maskování podezřelých aktivit
- Útok na aplikační vrstvě (L7 DDoS)

Zdroj: Nexusguard report 2020

Distribution of Attack Vectors

- UDP Attack (44.57%)
- DNS Amplification Attack(35.68%)
- UDP Fragmentation Attack(6.8%)
- CLDAP Reflection Attack(6.24%)
- SSDP Amplification Attack(3.87%)

Global	%
China	72.43%
Brazil	5.18%
Indonesia	2.93%
United States	2.72%
Thailand	2.29%
Taiwan	1.81%
Russian Federatior	1.51%

EMEA	%
Russian Federation	21.67%
France	13.79%
Turkey	9.35%
United Kingdom	8.63%
Ukraine	7.29%
Germany	4.74%

OCHRANA SÍŤOVÉHO PERIMETRU

DDoS Ochrana

- Důvod DDoSu → Cena
  - Nízká cena objednání
  - Vysoké škody
  - Drahá ochrana

Dark Web Price Index 2021

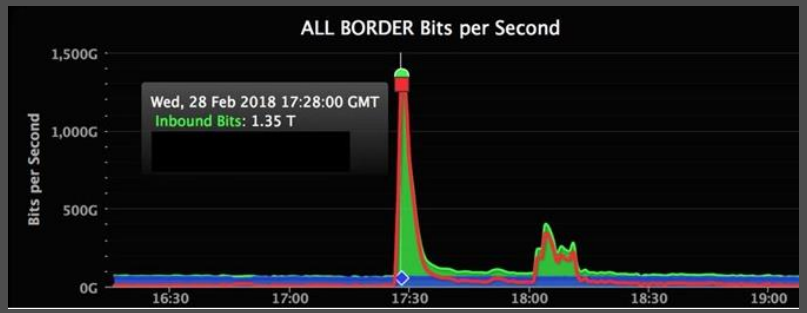
Credit card details, account balance up to $1000	**$12**
US driving license, high quality	$550
Hacked Instagram account	$55.45
LinkedIn followers x 1000	$10
Unprotected website, 10-50k requests per second, 1 hour	$10

OCHRANA SÍŤOVÉHO PERIMETRU

DDoS Ochrana

- Zajímavé útoky

- Útok na Github
  - 1,34 Tbps
  - Tisíce AS a desetitisíce zařízení
  - Detekce – 10 minut
  - Mitigace – 20 minut



- AWS DDoS (2020)
  - Největší
  - 2,34 Tbps

OCHRANA SÍŤOVÉHO PERIMETRU

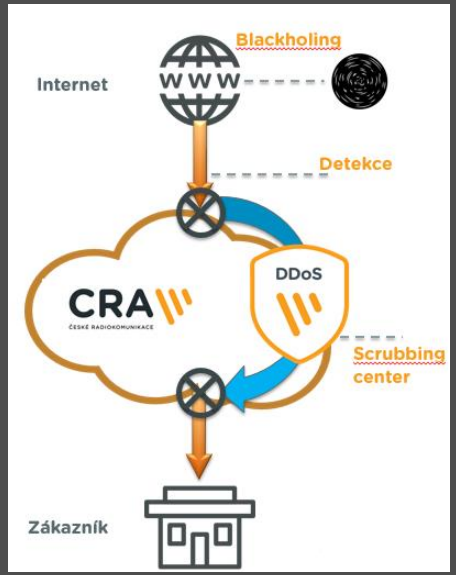
DDoS Ochrana

- Jak se chránit?

- Poskytovatel
  - Součást FENIX (NIX)

- Nastavení limitů provozu
  - Provoz CR/SK/Svět
  - TCP a ostatní provoz
  - Politiky provozu na FW
  - Limity

- DDoS detekce a čištění
  - Služba
  - Filtrování nežádoucího provozu



OCHRANA SÍŤOVÉHO PERIMETRU

Firewall

- První co stojí v cestě

- Attack Surface
  - Snížení rizika útoku
  - Pouze nutné IP adresy, porty, služby
  - Použité aplikace, šifry
  - Geolokace
  - Risk Assesment
  - Scanování a logování

- Hardening
  - Konfigurace
    - Přístupy
    - Limity provozu
  - Zranitelnosti
    - Patch, fix, WAF
  - Aktualizace
    - Kódu, šifer, certifikátů
  - Management přístupů a hesel
    - Least privilege

OCHRANA SÍŤOVÉHO PERIMETRU

Next-gen Firewall

- NAT není firewall
- Služby poskytované do Internetu
  - Pouze nutné protokoly

- Intrusion Detection/Prevention Systém

Detekce signatur
- Exploty
- Zranitelnosti

Detekce anomálií
- Překročení hodnot
- Nestandardní chování

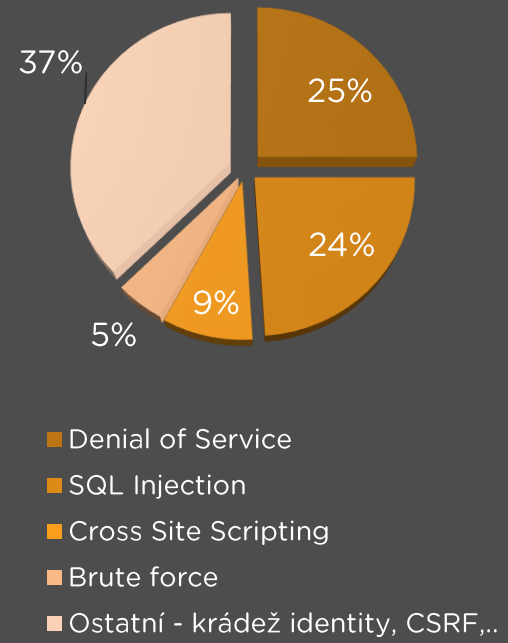
- Monitoring a upozornění
- Zablokování spojení, paketu
- Reset spojení

OCHRANA APLIKAČNÍ VRSTVY

Zranitelnosti aplikační vrstvy

	OWASP Top 10 - 2017
→	A1:2017-Injection
→	A2:2017-Broken Authentication
↘	A3:2017-Sensitive Data Exposure
U	A4:2017-XML External Entities (XXE) [NEW]
↘	A5:2017-Broken Access Control [Merged]
↗	A6:2017-Security Misconfiguration
U	A7:2017-Cross-Site Scripting (XSS)
☒	A8:2017-Insecure Deserialization [NEW, Community]
→	A9:2017-Using Components with Known Vulnerabilities
☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

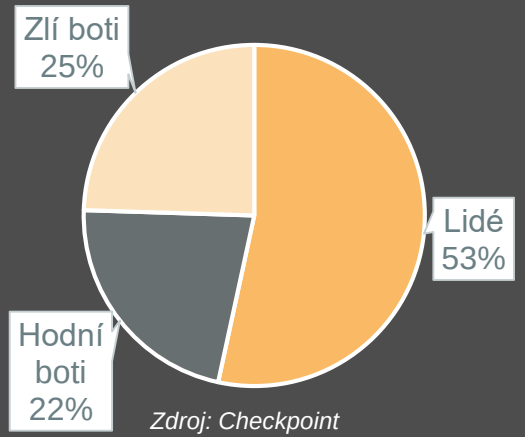
Nejčastější aplikační útoky



OCHRANA APLIKAČNÍ VRSTVY

ˇAutomaticky generovaný provoz

- BOTi na Internetu
  - Cca 25% internetového provozu
  - Vytížení back-end infrastruktury
  - Malé rychlosti
  - Těžko detekovatelné



Zdroj: Checkpoint

- Hodní boti
  - Vyhledávače
  - Webové crawlery
  - Srovnávače cen

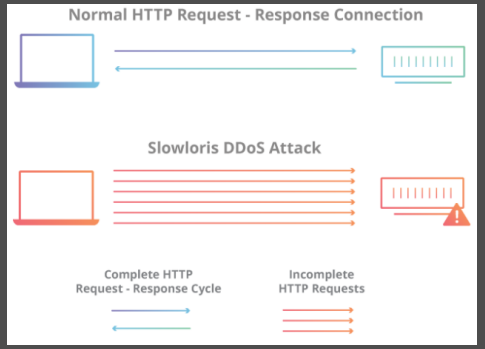
- Zlí boti
  - Data scrapping
  - DDoS útoky
  - Krádeže dat a identit

OCHRANA APLIKAČNÍ VRSTVY
L7 DDoS

- Rozdíl oproti L4
  - Zranitelnosti protokolů, aplikací (http)
  - Vytížení back-end infrastruktury
  - Malé rychlosti
  - Těžko detekovatelné

- U L7 DDoS stačí menší, někdy i neznatelný útok k vyřazení cílové služby

- Slowloris DDoS Attack



Zdroj: Cloudflare

OCHRANA APLIKAČNÍ VRSTVY

Možnosti obrany

- Secure by design
- Update/patchování
- Web Application Firewall (WAF)

Metody ochrany WAF

Zdroj: F5

- Detekce a mitigace
  - Počty spojení/requestů/transakcí
- Geolokace
- Zdrojové IP adresy
- Client-side integrity
  - Je to člověk?
- Capcha
- Rate limit
  - Omezení počtu požadavků
- Monitoring zatížení back-endu

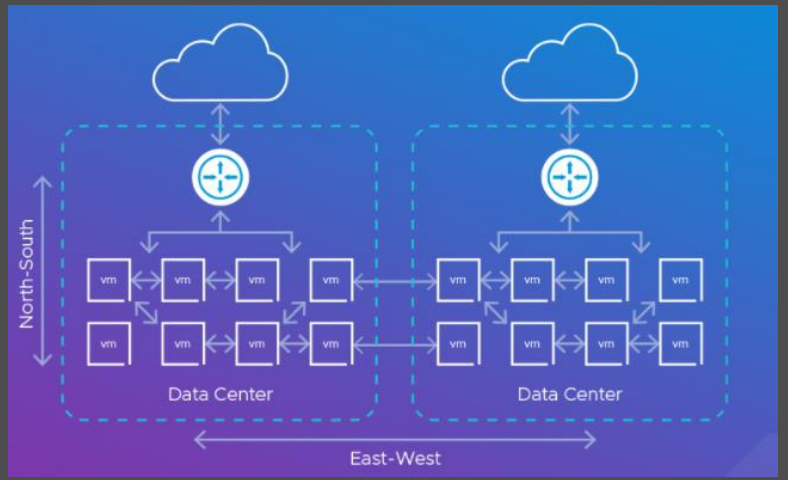
OCHRANA INFRASTRUKTURY

Mikrosegmentace

MIKROSEGMENTACE

Proč je důležitá

- Vytváříme „brány“ mezi různými světy/vrstvami
- Rozdělení do logických celků
  - Povolení business provozu
  - Nic navíc
  - Škálovatelné (odolné změnám)
  - (klientské sítě = vstupní brána Malware)
- Členění provozu
  - Flow Based
    - NetFlow
  - Content/Data based
    - Kritičnost dat



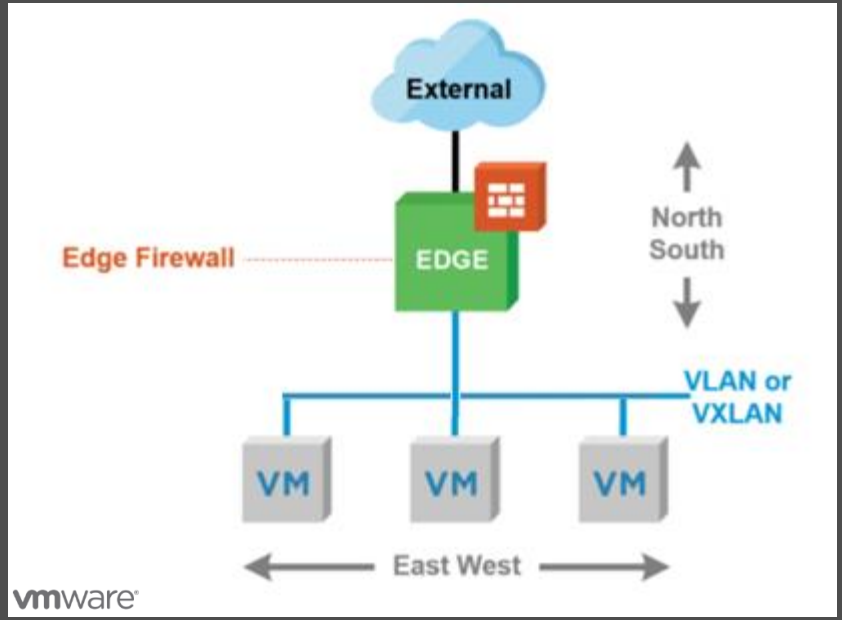
Zdroj: VMware

- Inter VM komunikace
- Segmentace sítě
- Zamezení laterálnímu pohybu

MIKROSEGMENTACE

Proč je důležitá

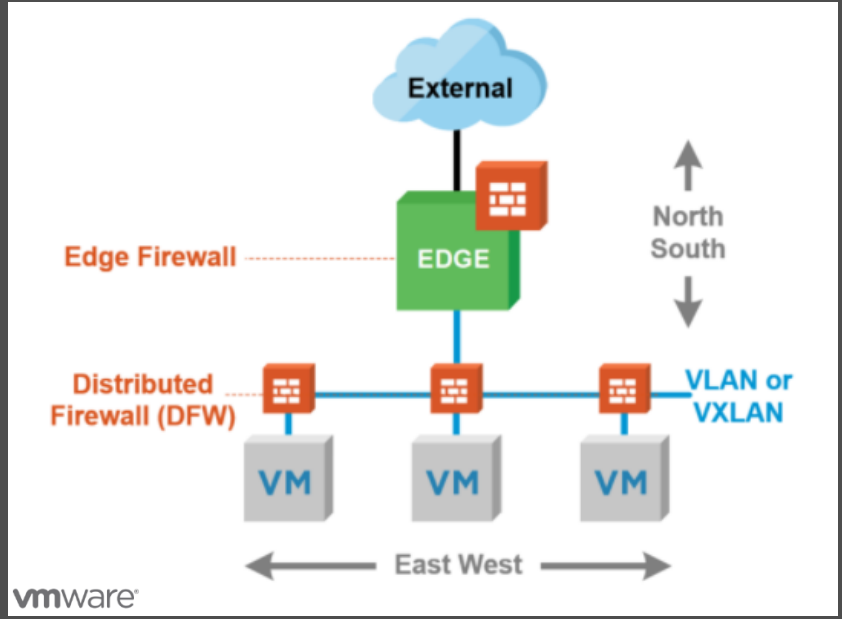
- Interní segmentační firewall
  - Lze využít Edge firewall
    - Provoz je směrován přes Edge
      - Kapacitní nároky



MIKROSEGMENTACE

Proč je důležitá

- SDN (software Defined Network) přístup
  - Eliminace North – South provozu
  - Distribuovaný Firewall
    - Požadavky:
      - Distribuovannost
      - Škálovatelnost
      - Výkon
      - Mobilita provozu
      - Detekce aplikací
      - Automatické politiky



PILÍŘE BEZPEČNOSTI V ONLINE SVĚTĚ

Základní členění bezpečnosti nejen v cloudovém světě

Detekce

- Flow monitoring
- Performance monitoring
- SIEM
- SOC
- Vulnerability management
- Account activity
- ML, AI

Incident response

- SIEM
- SOC
- EDR/XDR
- Automatizace

Správa uživatelů a přístupů

- Adresářové služby
- SSO
- PAM
- VPN

Ochrana infrastruktury

- DDoS Ochrana
- WAF
- Firewall
  - (next-gen)
- Mikrosegmentace
- VPN/ZTNA
- SASE

Ochrana dat

- Zálohování
- DR
- Ochrana před APT
- Sandboxing
- API Security

Compliance

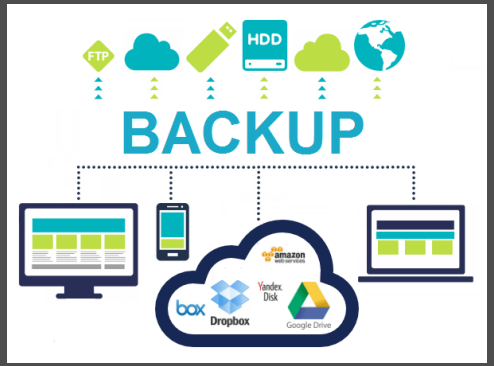
- Audity
- Směrnice
- Bezpečnostní politiky

OCHRANA CLOUDOVÉHO PROSTŘEDÍ

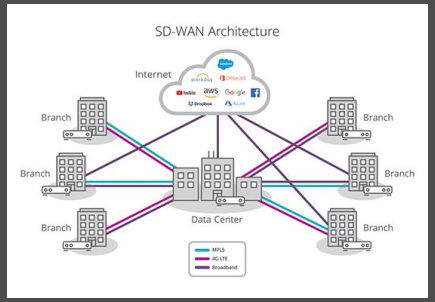
Co ještě pomáhá

CO DALŠÍHO VÁM S BEZPEČNOSTÍ POMŮŽE

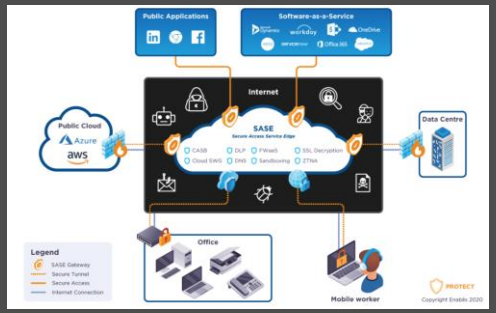
Standardně jsou útočníci o krok před námi – je tedy třeba myslet dopředu



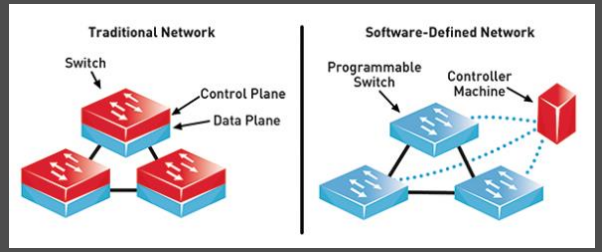
BACKUP



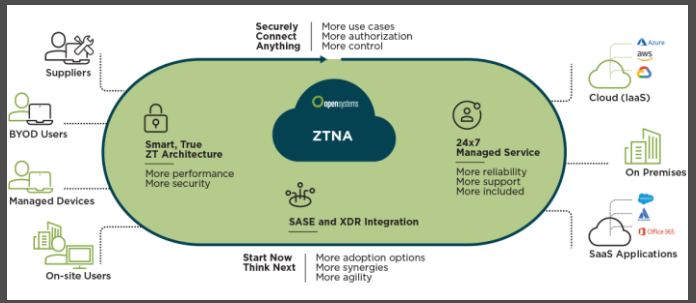
SD-WAN



SASE



SDN



ZTNA

KONTAKTY

V případě dotazů

Q & A – TENTOKRÁT OFFLINE

- Lukáš Bartakovič
  - Produkt manažer - Security
  - L.bartakovic@cra.cz
  - 733 140 278
- Marek Erneker
  - Produkt manažer - Cloud
  - M.erneker@cra.cz
  - 724 340 196

DĚKUJEME ZA POZORNOST