KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťová a komunikačná bezpečnosť

08 Architektúra bezpečnostnej brány

KCKB UPJS CSIRT UPJS

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Architektúra bezpečnostnej brány

- architektúra bezpečnostnej brány (firewall)
- demilitarizovaná zóna
- pravidlá filtrovania

Bezpečnostná brána (firewall)

- kontroluje a riadi prevádzku medzi sieťami s rôznou úrovňou dôvery
- vynucuje bezpečnostnú politiku organizácie
- funguje ako kontrolný bod na hranici počítačovejsiete (perimeter)
- môže byť hardvérová, softvérová alebo virtuálna
- základný, no nie jediný prvok ochrany počítačovej siete

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

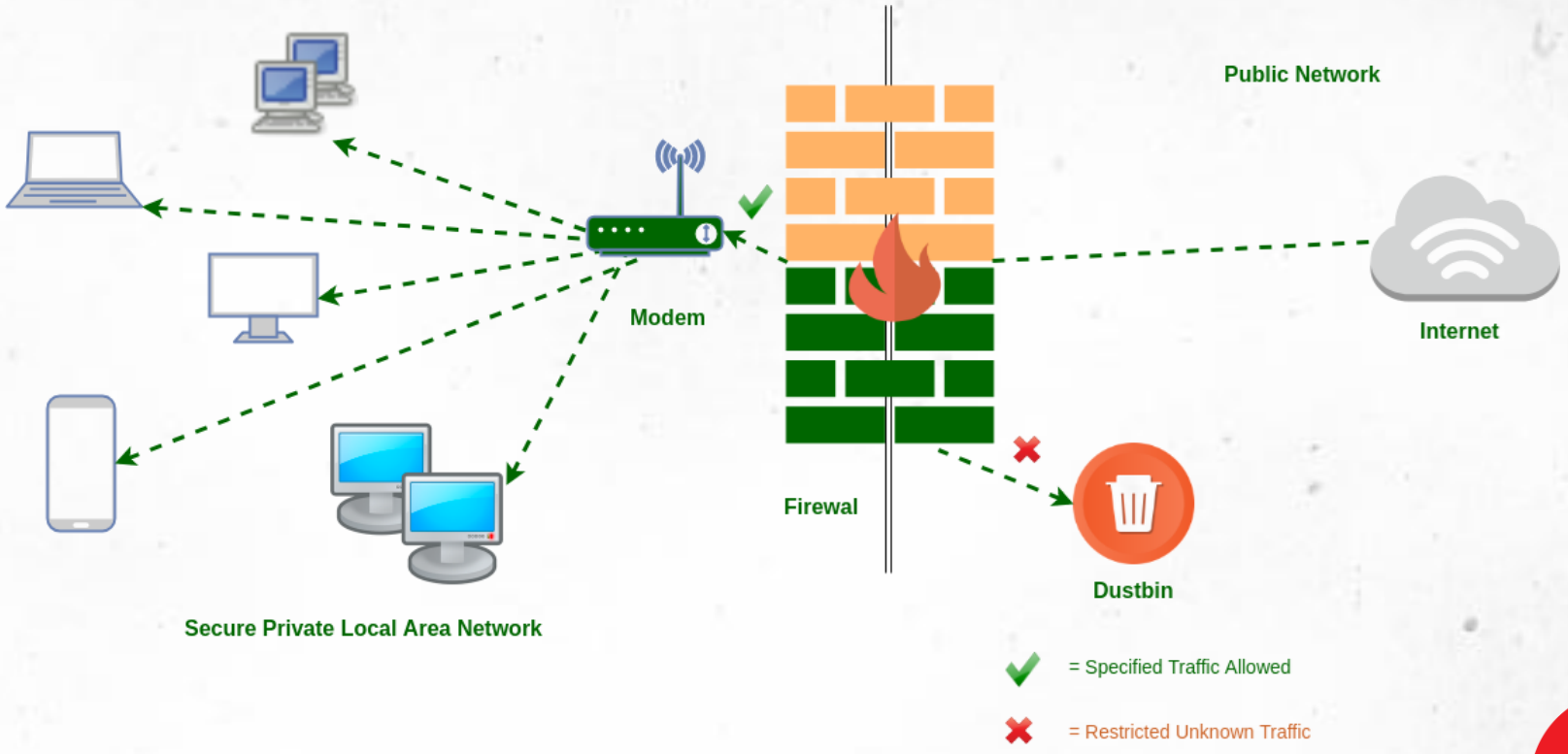
Typy firewallov (I.)

- paketový filter - rozhoduje podľa hlavičiek (IP, port, protokol)
- stavový firewall - sleduje stav spojení (connection tracking)
- aplikačná brána / proxy - kontrola na úrovni aplikácie
- NGFW (Next-Generation Firewall) - DPI, IPS, identita, aplikácie
- WAF - špecializovaný firewall pre webové aplikácie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Typy firewallov (II.)

- **paketový filter**



Zdroj: https://www.geeksforgeeks.org/computer-networks/types-of-firewall-and-possible-attacks/

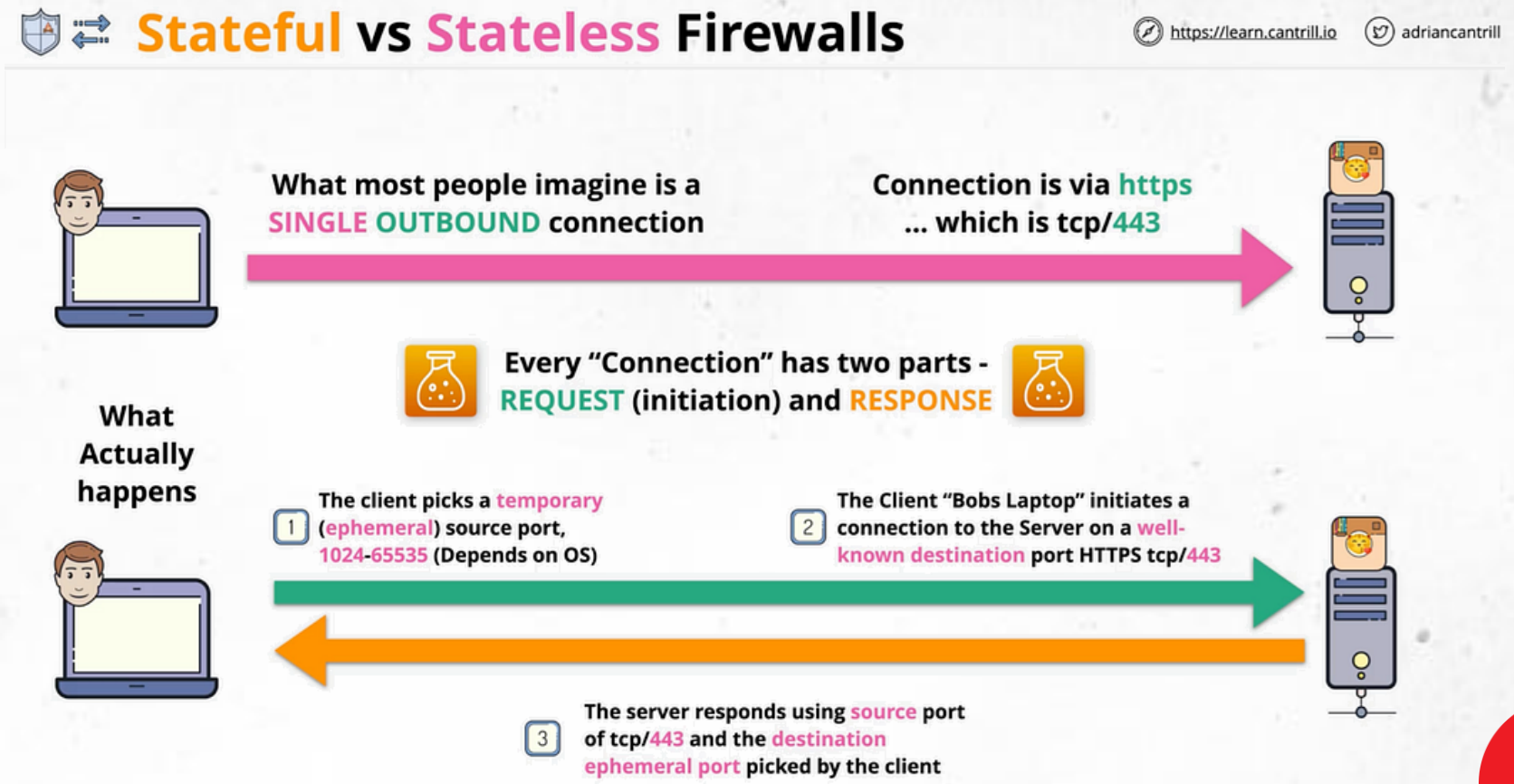
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Stavový vs. bezstavový filter (I.)

- **Bezstavový**
  - posudzuje každý paket samostatne
  - rýchly, ale ľahšie obíditeľný
- **Stavový**
  - udržiava tabuľku aktívnych spojení
  - rozlišuje nové a existujúce relácie
  - presnejšie rozhodovanie a vyššia bezpečnosť

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Stavový vs. bezstavový filter (II.)



Zdroj: https://walid-mahmoud.medium.com/osi-model-layer-7-stateful-stateless-firewalls-509d3d8c97f0

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Architektúry nasadenia FW

- bastion host - jeden silne zabezpečený verejný uzol
- screened host - router + firewall pred interným hostom
- screened subnet - dva firewally a oddelená DMZ
- viacúrovňová obrana (defense in depth)
- voľba podľa veľkosti, rizík a požiadaviek organizácie

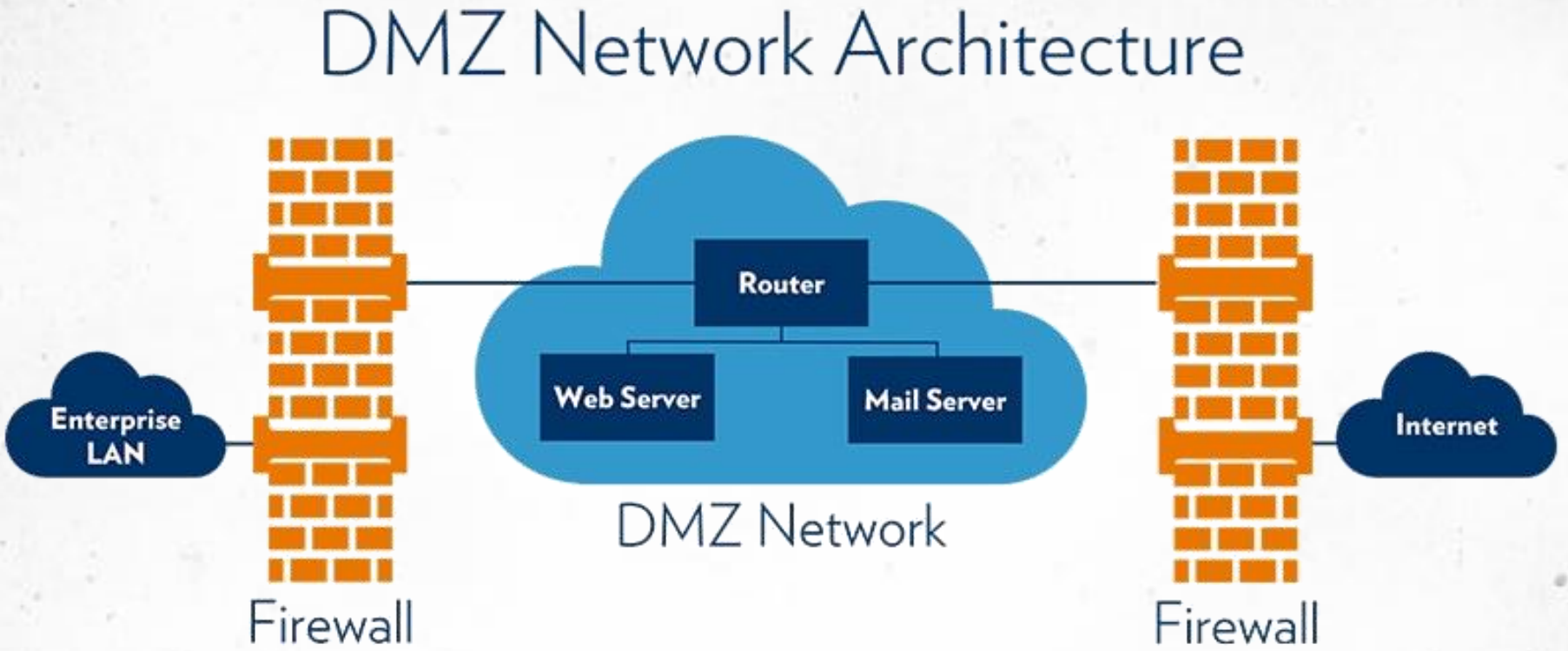
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Demilitarizovaná zóna (DMZ) (I.)

- oddelený segment medzi internetom a internou sieťou
- umiestnenie verejne dostupných služieb (web, mail, DNS)
- pri kompromitácii služby ostáva interná sieť chránená
- prístup do DMZ aj z DMZ je striktne filtrovaný
- realizovaná jedným alebo dvoma firewallmi

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Demilitarizovaná zóna (DMZ) (II.)



Zdroj: https://pages.rexelusa.com/blog/automation/idmz

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Demilitarizovaná zóna (DMZ) (III.)

- **Princípy návrhu DMZ**
  - z internetu povolený prístup len k publikovaným službám
  - z DMZ do internej siete len nevyhnutné, presne definované spojenia
  - servery v DMZ s minimom služieb (hardening)
  - oddelené sieťové segmenty a VLAN
  - logovanie a monitoring všetkých prechodov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Pravidlá filtrovania

- pravidlo definuje: zdroj, cieľ, protokol, port a akciu
- akcie: PERMIT (povoliť), DENY/DROP (zahodiť), REJECT
- pravidlá sa vyhodnocujú zhora nadol (poradie je dôležité)
- princíp implicitného zákazu (default deny)
- povoľuje sa len to, čo je výslovne potrebné (least privilege)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Tvorba a správa pravidiel

- špecifické pravidlá pred všeobecné
- pravidelná revízia a odstraňovanie nepotrebných pravidiel
- dokumentácia účelu každého pravidla
- riadenie zmien (change management)
- testovanie pred nasadením do produkcie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezpečnostné riziká

- príliš voľné pravidlá typu „any-any“
- neaktuálne pravidlá pre už zrušené služby
- nesprávne poradie pravidiel
- chýbajúce logovanie zahodených paketov
- spoliehanie sa len na firewall (chýba viacvrstvová ochrana)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Firewall ako súčasť obrany

- kombinácia s IDS/IPS na detekciu a prevenciu prienikov
- integrácia s SIEM pre korelovanie udalostí
- segmentácia internej siete (mikrosegmentácia)
- VPN brána pre bezpečný vzdialený prístup
- pravidelné aktualizácie firmvéru a signatúr

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Analýza firewall logov (I.)

- Firewall log je často prvý signál, ktorý analytik vidí v SIEMe. Cieľom nie je iba prečítať riadok, ale okamžite pochopiť, čo sa stalo.

- Schopnosť čítať raw firewall logy je základná SOC zručnosť, nie pokročilá špecializácia.
- Najprv určujeme, či bola prevádzka povolená alebo zablokovaná.
- Dôležité je rozlíšiť smer komunikácie: inbound, outbound alebo laterálny pohyb.
- Jeden riadok logu dáva kontext; séria logov ukazuje vzor správania.
- Firewall logy treba korelovať s EDR, Windows Event Logs, DNS a autentifikačnými logmi.

Pracovná otázka analytika

„Čo sa pokúsilo komunikovať, kam, cez akú službu, s akým výsledkom a či sa to opakuje?“

Zdroj: https://medium.com/@jbird24/how-to-read-firewall-logs-for-soc-analysts-what-you-are-expected-to-know-94a9c5fbcc55

Analýza firewall logov (II.)

- Anatómia firewall záznamu (logu)

```
2024-03-15 14:23:45  ALLOW  TCP  10.0.0.50:49832  →  93.184.216.34:443
Rule: Web-Access-Out  Zone: Trust → Untrust  Sent: 1,245  Received: 45,678  Duration: 32s
```

Timestamp

Kedy sa udalosť stala. Overiť UTC vs. lokálny čas.

Action

ALLOW znamená úspešnú komunikáciu; DENY/DROP zablokovanie.

Source → Destination

Kto komunikoval s kým a na aký port/službu.

Rule & Zone

Ktoré pravidlo rozhodlo a aký bol smer prevádzky.

Bytes

Pomer odoslaných a prijatých dát môže indikovať exfiltráciu.

Duration

Krátke série môžu indikovať scan; pravidelné intervaly beaconing.

Analýza firewall logov (III.)

- **Vzory správania / útokov vo firewall záznamov (logov)**

Port scanning

Jedna IP skúša veľa portov alebo jeden port na mnohých cieľoch.

1 zdroj → veľa portov

C2 beaconing

Rovnaký cieľ, rovnaký interval, podobná veľkosť a krátke trvanie.

5 min intervaly

Data exfiltration

Veľké objemy dát smerom von, málo dát späť, často mimo pracovného času.

Sent ≫ Received

Brute force

Séria krátkych spojení, potom dlhšie spojenie s vyšším objemom dát.

krátke pokusy → úspech

Analýza firewall logov (IV.)

- **DROP vs DENY**

Rovnaké jadro dát, iný zápis

Palo Alto	CSV, traffic vs. threat logs, session end reason, pre/post NAT
FortiGate	key=value formát, proto=6/17/1 pre TCP/UDP/ICMP
Cisco ASA	message ID, napr. 302013 built, 106023 denied ACL
iptables / cloud	SRC/DST/SPT/DPT; flow logs často iba metadata bez payloadu

DROP vs. DENY

DENY

Firewall pošle odpoveď späť zdroju, napr. ICMP unreachable alebo TCP RST.

DROP

Firewall paket potichu zahodí. Útočník nedostane potvrdenie, či cieľ existuje.

- Pre externú prevádzku je DROP často bezpečnejší, lebo prezrádza menej informácií.
- Pre interných používateľov môže byť DENY praktickejší, pretože poskytne okamžitú chybu.
- Pri vyšetrovaní je dôležité zistiť, či bola komunikácia iba pokusom, alebo reálne prešla.

Analýza firewall logov (V.)

- **Checklist – analýza firewall záznamu (logu)**

1	**Action**	ALLOW je vyššia priorita ako DENY/DROP pri podozrivom cieli.
2	**Direction**	Untrust → Trust a DMZ → Trust preveriť okamžite.
3	**IP & TI**	Interná/externá IP, reputácia: VirusTotal, AbuseIPDB, GreyNoise.
4	**Port/service**	443 môže byť web, ale aj C2; 22/3389/445 sú citlivé.
5	**Volume & timing**	Sent/Received pomer, pravidelné intervaly, čas mimo pracovných hodín.
6	**Correlation**	Doplniť EDR, DNS, autentifikačné logy a endpoint udalosti.

Zdroj: https://medium.com/@jbird24/how-to-read-firewall-logs-for-soc-analysts-what-you-are-expected-to-know-94a9c5fbcc55

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť