Hacking **war** stories

Intermax - 04/12/2019

Introductie

Korte Introductie

whoami

```
Mischa-NFIR:~ mischa-nfir$
```

Korte Introductie

Achtergrondinformatie

- IT Beveiligingsonderzoeker bij NFIR
- 1700+ meldingen gedaan naar organisaties in de 5 jaar
- 7+ jaar ervaring in ICT (Madison Gurkha, Sogeti, RoS)
- Help organisaties om inzicht te krijgen in hun digitale kwetsbaarheden
- Geef inzicht door middel van awareness sessies

Inzicht bieden in digitale beveiligingsrisico's voor jou
(en de organisatie waar jij werkt)

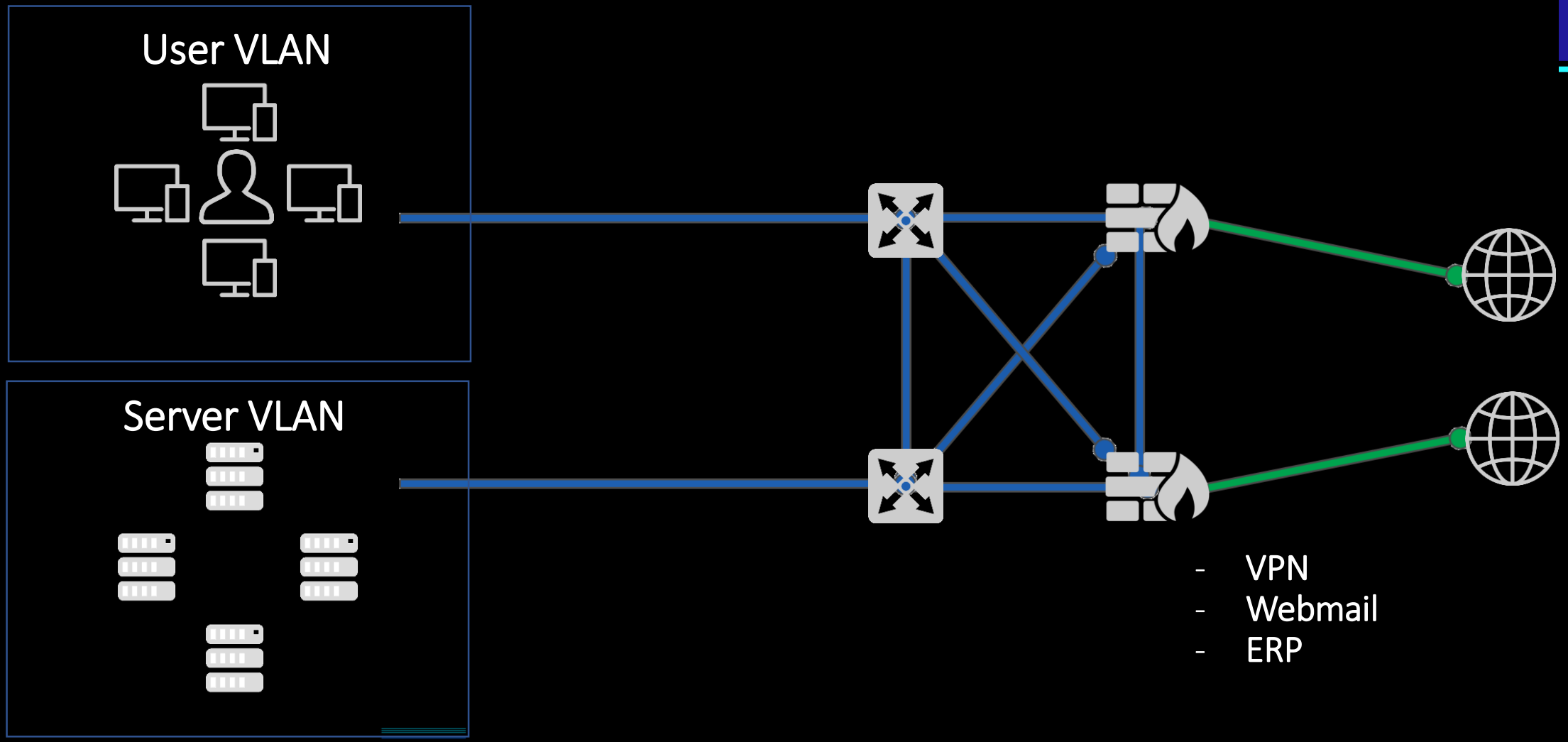
Wie heeft hier wel eens een hack meegemaakt?

De casus

De casus

- Organisatie die **wereldwijd** actief is
- Paar honderd FTE
- Actief op het gebied van handel in goederen
- IT-infrastructuur in meerdere landen

Netwerk-omgeving



Maandag –

De IT Manager ontvangt op zijn privé-email een bericht van een onbekend persoon - In het bericht staat:

“Wij hebben bij je ingebroken - mail ons vandaag voor 12:00 terug – of we zullen laten zien waar we toe in staat zijn.” (vertaling)

Maandag –

De IT Manager leest zijn e-mail, schrikt en belt met de systeembeheerder

De systeembeheerder:
‘het zal wel om spam gaan, maak je geen zorgen’

Maandag – 12:00 tot Dinsdag 12:00

Geen ongewone activiteit op het netwerk

Dinsdag 12:17 – Begin Incident

- Firewall geeft via e-mails waarschuwingen naar beheerders over verbindingen naar buiten (poort 22)
- Servers zijn trager geworden (meldingen van gebruikers)
- Bestandsserver is ontoegankelijk (conclusie beheerder)
- Een van de servers met het ERP pakket (Windows server 2003) blijkt continu opnieuw opstarten

Donderdag 16:00

- IT Manager wordt door systeembeheerders verteld dat ze het niet opgelost krijgen
- IT Manager vraagt intern documentatie op over verantwoordelijke leveranciers van de firewalls
- IT Manager geeft opdracht aan beheerders om uit te zoeken welke diensten er naar buiten open staan en wat er met de bestandsservers aan de hand is

Welke acties hadden er nog meer kunnen worden genomen?

Donderdag 20:00

- Systeembeheerders rapporteren terug aan de IT Manager:
  - De bestanden op de bestandsservers blijken versleuteld
    - Met ransomware
    - Onbekend hoe binnengekomen
    - Back-ups zijn deels versleuteld
- Er blijkt geen overzicht te zijn van de openstaande diensten aan het internet

Vraag voor de zaal:
Wat is de **beste** actie om nu te nemen?

De IT Manager

- Brengt de CEO op de hoogte
- Belt het NFIR Incident Response-team (IR)

Donderdag 21:00

IR-team komt op locatie

- Intake met betrokkenen
  - Welke acties zijn er al uitgevoerd
  - Welke servers zijn er mogelijk geraakt
  - Welke capaciteit is er beschikbaar vanuit de eigen organisatie

Informatie van Systeembeheer

- VPN-servers is volgens de beheerders gehackt
- Bestandsserver is versleuteld
- Poorten zijn dichtgezet
- Geen back-up terug gezet
- Virtuele machines uitgezet (Nooit doen!)

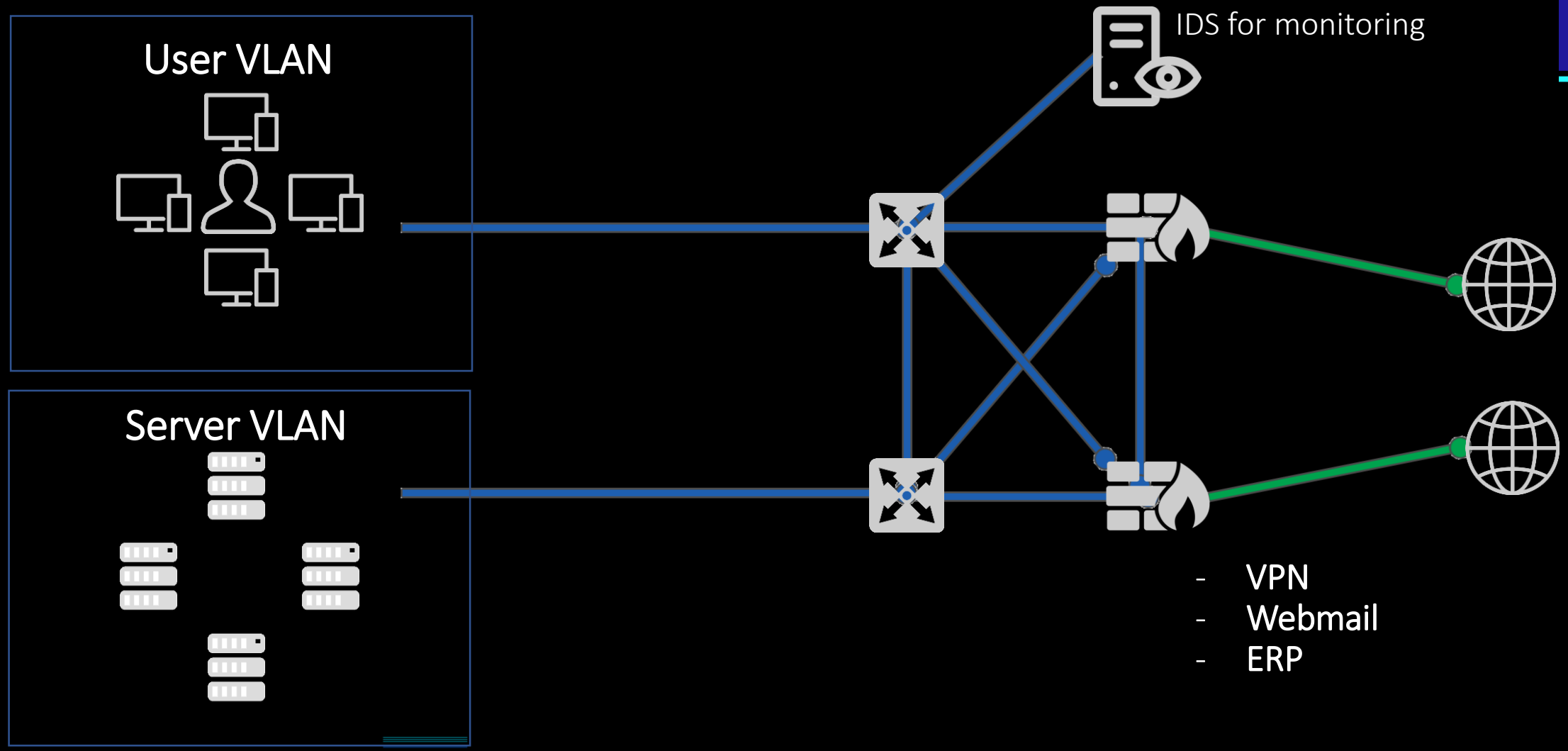
Verdeling taken binnen IR-team

- Taakverdeling binnen IR-team
  - Forensisch onderzoekers
    - Veiligstellen en onderzoeken
  - Ethische Hackers
    - Zoeken naar patient-zero
    - Beschermen van het netwerk
  - Projectlead
    - Communicatie, Ondersteuning

Acties binnen IR-team

- Installeren IDS oplossing om grip te krijgen
- Veilligstellen van informatie
- Onderzoeken van informatie
- Het vaststellen van de getroffen machines
- Het vaststellen van aanwezige security scanners
- Het actief samenwerken met beheerders om risico's en aanvallen te mitigeren

Netwerk-omgeving

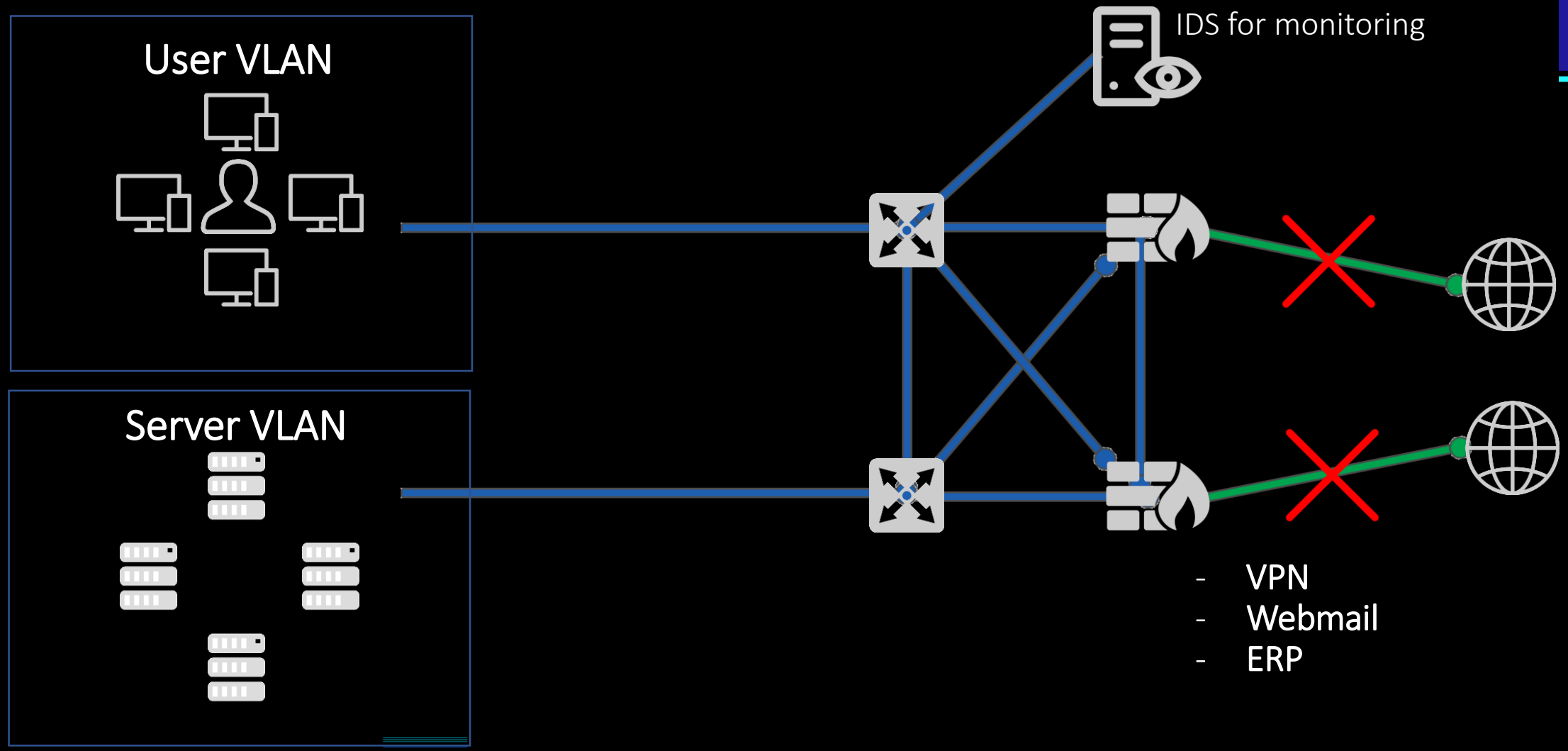


- VPN
- Webmail
- ERP

Incident Response acties

- Uitschakelen internetverbinding
- Vaststellen van de Indicators of Compromise (IoC’s)
- Dichtzetten van bekende risicovolle poorten in de firewalls

Netwerk-omgeving



Zaterdag – 14:00

Patient Zero

- Patient zero gevonden
- Bestandsserver aan het internet
- EternalBlue-exploit gebruikt

EternalBlue

- Exploit ontwikkeld door de NSA
- Gelekt door de Shadow Brokers Groep
- Kan zonder authenticatie tot het hoogste niveau toegang verkrijgen

EternalBlue

- Detecteerbaar door IDS
- Verdere uitbraak proberen te voorkomen

Vraag voor de zaal:
Wat is de **beste** actie om nu te nemen?

Incident Respons

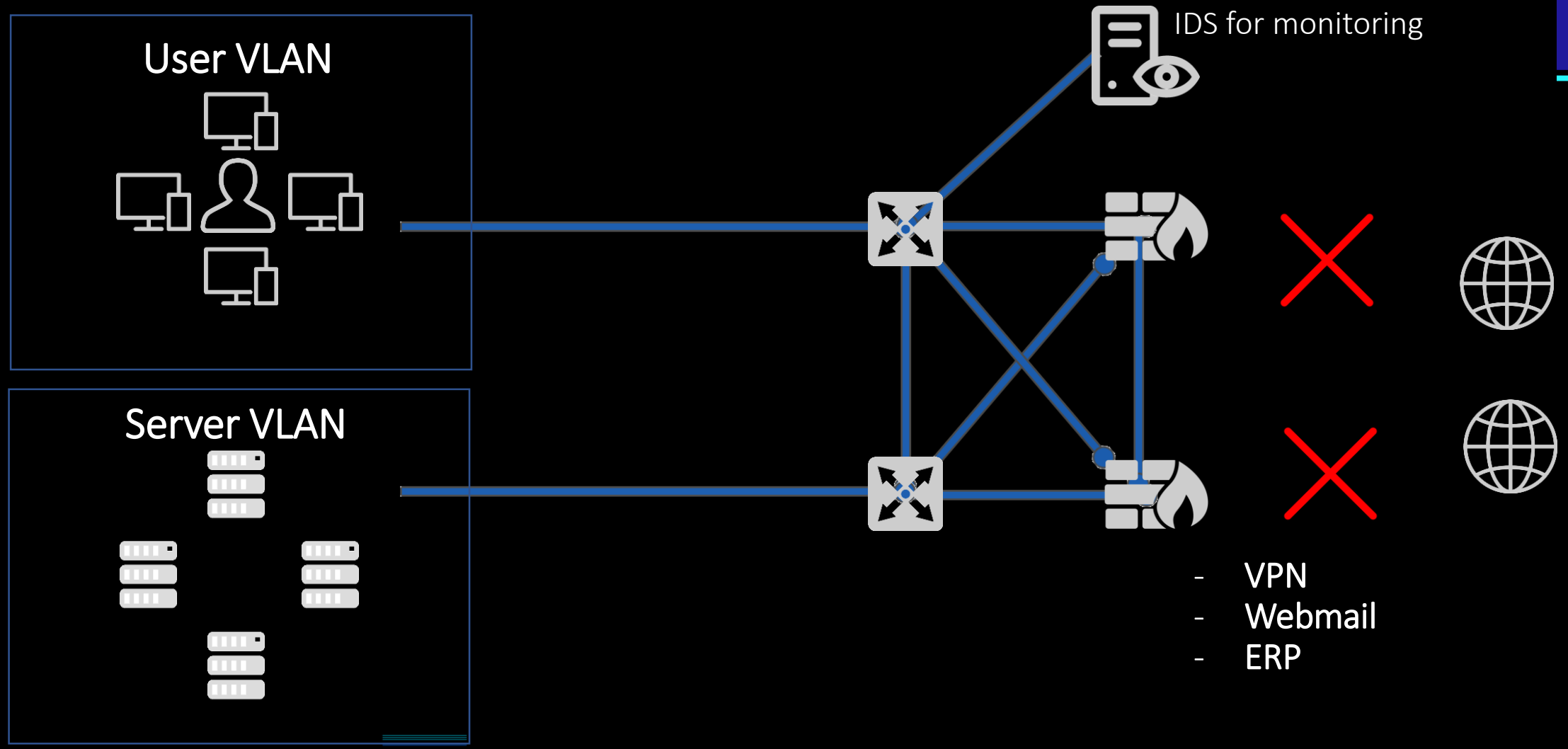
- Checklist opstellen voor getroffen machines
- Schoonmaken, updaten en herconfigureren
  - Zijn de machines schoon?
    - Controle op Indicators of Compromise
  - Als de machines schoon verklaard zijn
    - Beheerders de machines laten updaten
    - Beheerders de machines laten herconfigureren
    - Beheerders de checklists laten afvinken per machine

Forensisch onderzoek

Forensisch Onderzoek

- Onderzoek vindt verder plaats in het forensisch lab
- Onderzoek naar alle veilliggestelde machines
  - Gebruikte malware
  - Privilege escalatie
- Onderzoek naar veilliggestelde logs (firewall, windows logs)
- Reproduceren van de kwetsbaarheid welke misbruikt is
- Bevindingen vastleggen in een Rapportage

Netwerk-omgeving



Overzicht

- Het incident heeft zelf 14 dagen in totaal voortgeduurd
- Het forensisch onderzoek heeft 4 weken geduurd
- Er waren in totaal 20 machines gehackt
- De machines bleken al 3 weken geïnfecteerd te zijn

Lessons learned

- Escaleer op tijd – om erger te voorkomen
- Voer preventieve controles uit (pentesting, scanning)
- Zorg voor een duidelijk overzicht van openstaande diensten
- Bereid je voor op een incident
  - Incident Respons plan
  - Training

Vragen?

Hulp nodig?

088 – 32 30 205

www.nfir.nl

Bedankt voor jullie tijd