COMBIS KONFERENCIJA 13

VODICE
30. – 31.05.
2019.

Jeste li sigurni da ste sigurni?

Igor Klak, ITIL, CISA, ISO27k LA

Combis

Informacijska sigurnost

- Sustavni i holistički pristup ISMS – ISO 27001:2013
- GDPR
- ZKS
- Rasprave u USA kongresu
- Rasprave u Davosu – G20
- Nova EU Cybersecurity strategija
- Autorska prava na internetu
- Sigurnost kao jedan od tri stupa RH predsjedanja EU

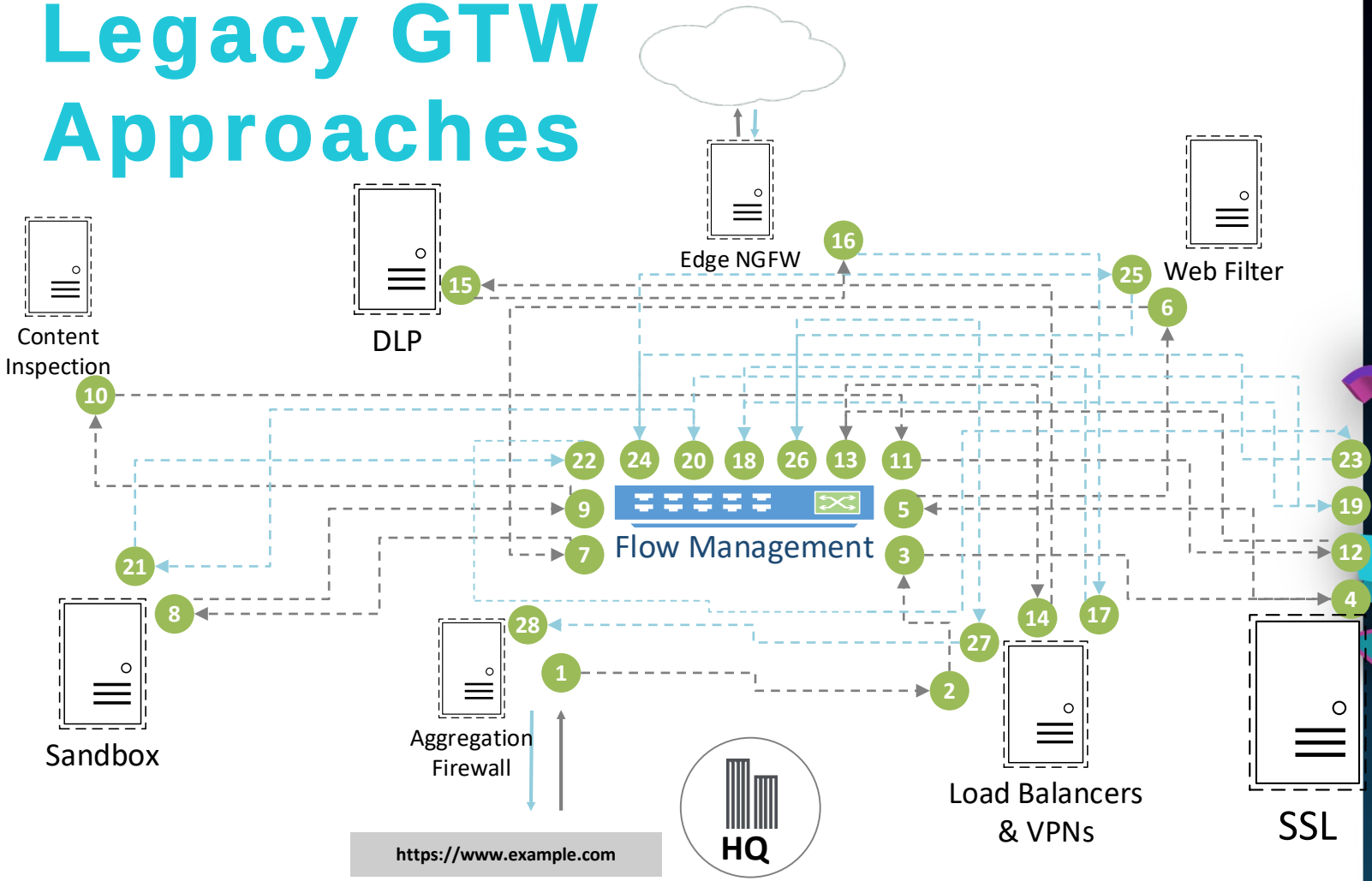
Podrška najvišeg rukovodstva

- Sigurnosni odjeli pridruženi Upravi
- Ukupni trošak cyber napada u 2018. godini

  50 MILIJARDI € samo u Njemačkoj
- Stanje u cyberspace:
  - 87% kompanija u Njemačkoj napadnuto u 2018. godini (porast od 33%)
  - NASA-i ukradeni podaci o zaposlenicima
    - Otkriveno u listopadu 2018.
    - Objavljeno u prosincu 2018. – prilikom objave nisu
      bili sigurni koliko i koji podaci su ukradeni
  - Značajan porast napada – izvor DT centrala u Bonnu
    - 2017. 4 M napada u danu
    - 2018. 12 M napada u danu
    - Početak 2019. 24 M napada u danu
    - U ožujku 2019. 32 M napada u danu

Crime	Annual Revenues
Illegal online markets	$860 Billion
Trade secret, IP theft	$500 Billion
Data Trading	$160 Billion
Crime-ware/CaaS	$1.6 Billion
Ransomware	$1 Billion
Total Cybercrime Revenues	$1.5 Trillion

Legacy GTW Approaches



Managed Security Services

- Usluga umjesto opreme
- Fiksni mjesečni trošak na duže razdoblje
- Podrška u stručnoj pomoći – nedostatak stručnog kadra
- Softver na virtualnim platformama umjesto appliance-a
- Integracija prema Vašim potrebama
- Uska suradnja sa tehničkim timovima enterprise vendora
- Suradnja community-a
- Komponente: AV/EDR, NGFW, SIEM, vulnerability scan, e-mail security, DNS filtering

SIEM Rules

- Incident management vs. Incident response
- **Threat Intelligence - Phishing URLs, Malware URLs, potential Spam or Phishing sender, potential Botnet communication**
- **User locked out two times in 30min, Login Failure to Expired Account, Multiple Login Failures for Single Username, Login Failures Followed By Success to the same Username, Multiple Login Failures to the Same Destination**
- **Excessive Firewall Denies from Single Source**
- **Malware or Virus Clean Failed**
- **Remote Access from Foreign Country/Region**
- **Potential Local Port Scan Detected**
  - Events with the same source IP more than 5 times, across more than 100 destination port within 3 minutes
- **Long Duration Flow Detected**
- **Local Flood (TCP)**
  - *Detects when a single local host sends a large number of packets (greater than ....1500pps.....) to an internet destination over a small period of time. The packet rate in this rule can be adjusted as needed to reflect the network*

PLATINUM SPONZOR:
PLATINUM SPONSOR:

ZLATNI SPONZOR:
GOLD SPONSOR:

SREBRNI SPONZOR:
SILVER SPONSOR:

SPONZOR:
SPONSOR:

MEDIJSKI POKROVITELJ:
MEDIA SPONSOR:

COMBIS KONFERENCIJA 13

VODICE
30. – 31.05.
2019.

Hvala na pažnji!

Thank you for your attention!