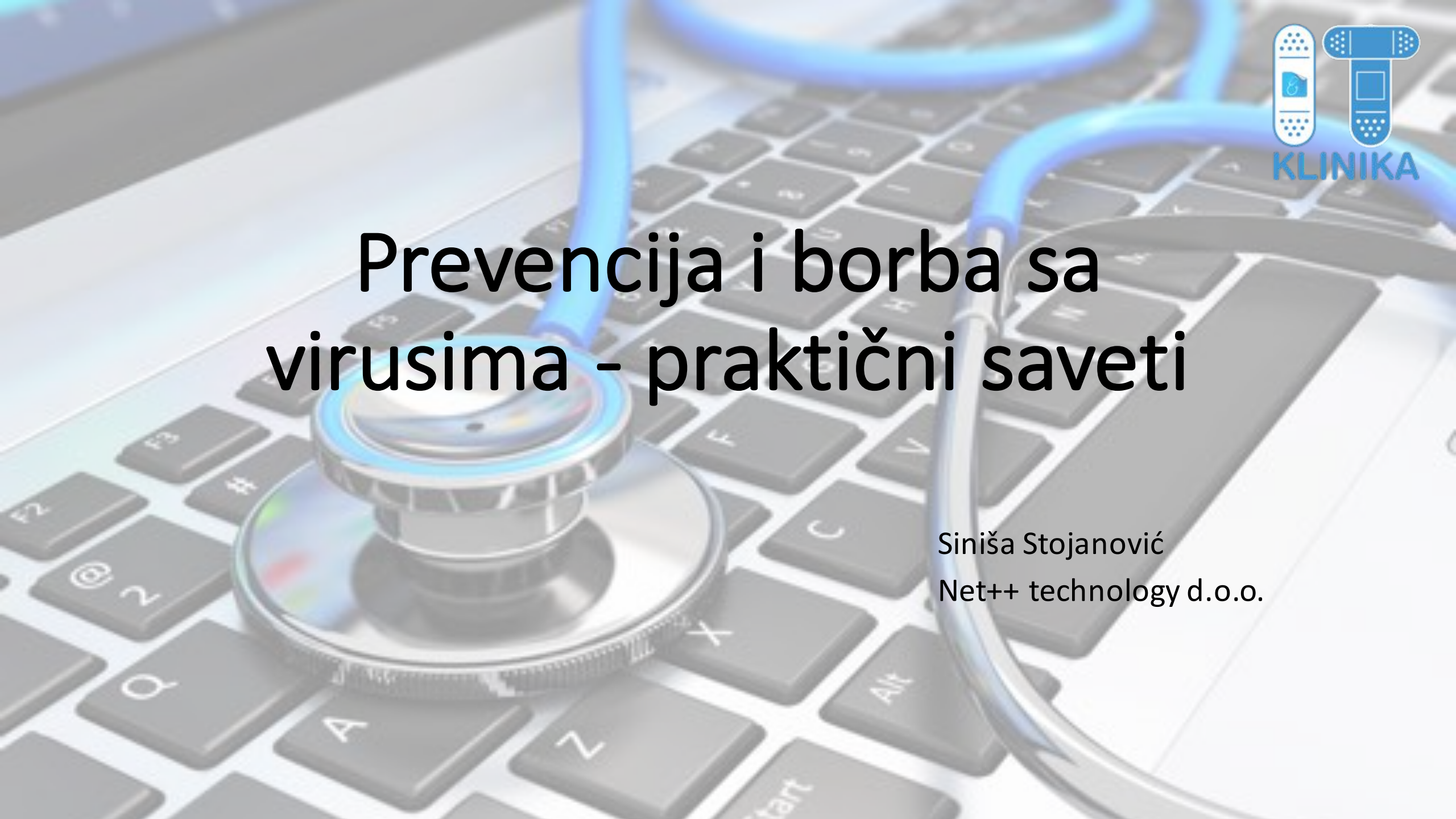


Prevencija i borba sa virusima - praktični saveti

Siniša Stojanović
Net++ technology d.o.o.

Današnje pretnje i napadi

- ***Hackers*** – ljudi sa veoma dobrim poznavanjem tehnologije i koji svoje znanje koriste za napade na računare drugih ljudi
  - ***White-hat hackers***
  - ***Black-hat hackers***
  - ***Hactivists***
  - ***Script kiddies*** ili ***script bunnies***
  - ***Cracker***
  - ***Cyberterrorists***

Današnje pretnje i napadi

- ***Malicious code***
- ***Hoaxes***
- ***Spoofing***
- ***Sniffer***

Današnje pretnje i napadi

- ***Worm (crv)***
- ***Denial-of-service attack (DoS)***
- ***Distributed denial-of-service attack (DDoS)***
- ***Trojan-horse virus***
- ***Backdoor programs***
- ***Polymorphic viruses and worms***

Današnje pretnje i napadi

KLINIKA

Attackers Moving Faster

5 of 6 large companies attacked

317M new malware created

1M new threats daily

60% of attacks targeted SMEs

Digital extortion on the rise

113% increase in ransom ware

45X more devices held hostage

Malware gets smarter

28% of malware was Virtual Machine Aware

Zero-Day Threats

24 all-time high

Top 5 unpatched for **295** days

Many Sectors Under Attack

Healthcare **+ 37%**

Retail **+11%**

Education **+10%**

Government **+8%**

Financial **+6%**

Antivirus is dead...

Brian Dye

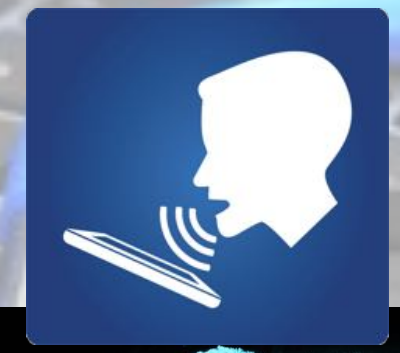
Symantec's senior vice president for information security in a weekend interview with The Wall Street Journal

Primarne bezbedonosne zone

- Autentifikacija i autorizacija
- Prevencija i otpornost na pretnje
- Detekcija i odgovor na pretnje

Autentifikacija i autorizacija

- Autentifikacija – potvrda korisnikovog identiteta
- Najsigurniji metodi autentifikacije:
  - User ID i password
  - Smart card ili token
  - Fingerprint ili voice signature
  - Mobilni uređaj i PIN



Prevencija i otpornost

- Tehnologije dostupne kako bi pomogle u prevenciji i izgradile otpornost na napade uključuju:
  - Content filtering
  - Encryption
  - Firewalls

Content Filtering

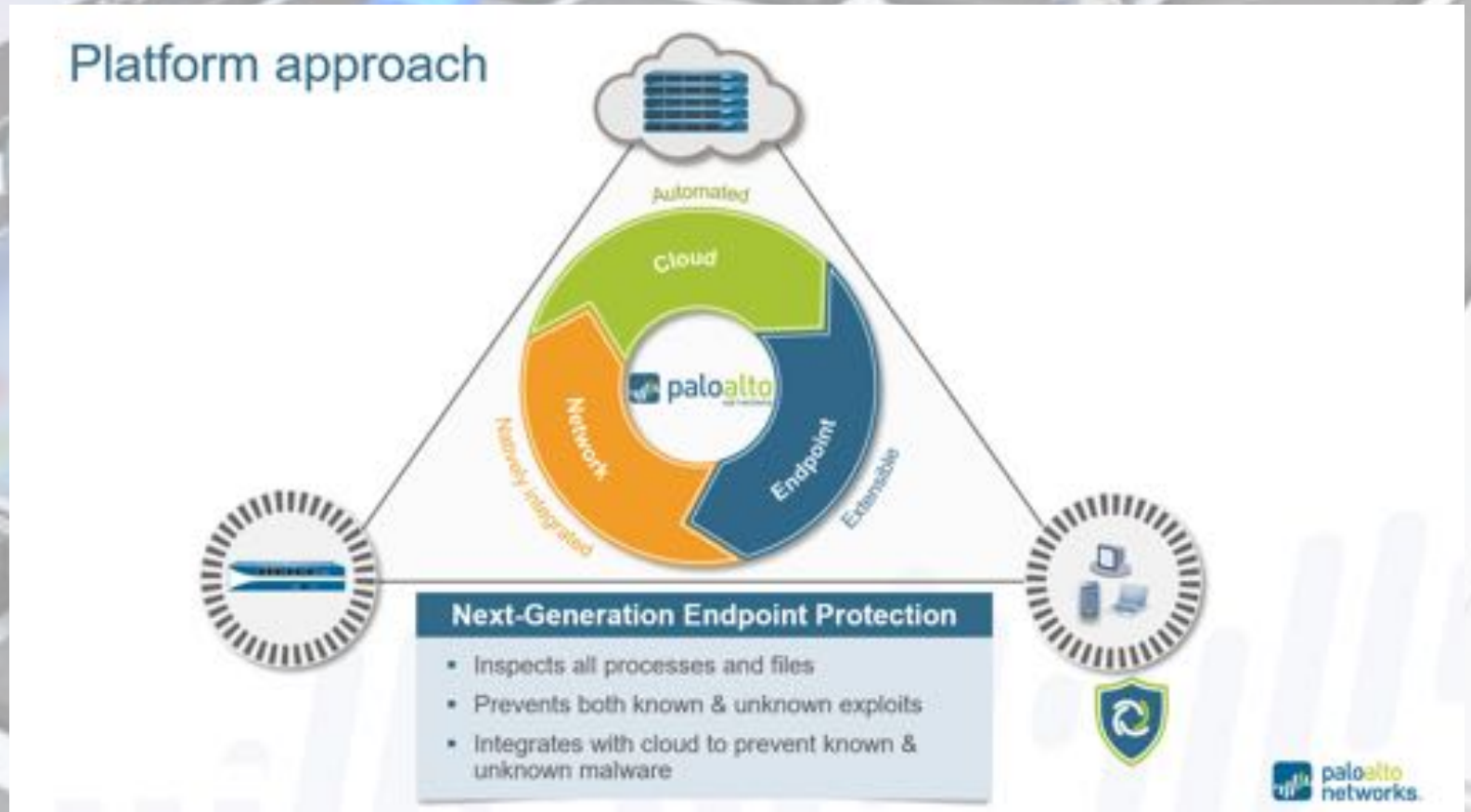
- Content filtering – softver kojim se filtrira transmisija neautorizovanih informacija
- Filtriranje e-mail poruka
- Sprečavanje da e-mail sadrži osetljive podatke
- Stopiranje spam-a
- Stopiranje virusa i njihovog širenja

Enkripcija

- U slučaju da dođe do povrede bezbednosti i krađe podataka, ukoliko su podaci kriptovani osoba koja ih krade neće biti u mogućnosti da ih koristi

Firewalls

- Firewall pretstavlja jedan od najčešćih načina za odbranju od pretnji i narušavanja bezbednosti



Detekcija i sanacija pretnje

- U slučaju da strategije prevencije i otpornosti budu zaobiđene u tom trenutku dolazi do proboja

- U ovom slučaju je potrebno da organizacija poseduje sistem za detekciju i sanaciju kako bi se sprečilo propagiranje eventualno napravljene štete

- Antivirusni softver je najčešći tip tehnologije detekcije i sanacije

Ljudski faktor

- Oko 33% incidenata imaju poreklo unutar organizacije
- E-mail
- Obaveštenost
- Saradnja

KLINIKA

Zaključak

1. OBEZBEDITE ŠTO BOLJE ANTI-MALVER REŠENJE
2. PATCH MANAGEMENT – UPRAVLJANJE AŽURIRANJEM APLIKACIJAMA I OPERATIVNIM SISTEMIMA
3. OGRANIČITE PRIVILEGIJE ADMINISTRATORIMA, OPERATIVNIM SISTEMIMA I APLIKACIJAMA
4. OGRANIČITE KORIŠĆENJE KORISNIČKIH APLIKACIJA
5. URADITE SEGMENTACIJU LOKALNE MREŽE I UVEDITE FIREWALL SLEDEĆE GENERACIJE

Zaključak

6. ZAŠTITITE E-MAIL I WEB SAOBRAĆAJ
7. DINAMIČKA ANALIZA POTENCIJALNIH MALVERA IZVRŠAVANJEM U SANDBOX-U
8. UVEDITE SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) ILI BAR LOG MANAGEMENT
9. KRIPTUJTE POVERLJIVE PODATKE/SISTEME
10. UVEDITE VIŠEFAKTORNU AUTENTIFIKACIJU
11. OBUČITE ZAPOSLENE O OSNOVAMA IT BEZBEDNOSTI

HVALA NA PAŽNJI