Varnostne grožnje in tveganja v informacijskih sistemih javne in državne uprave

Vladimir Ban
Direktor prodaje, Astec d.o.o.

Smo ali nismo ogroženi?

astec varne komunikacije

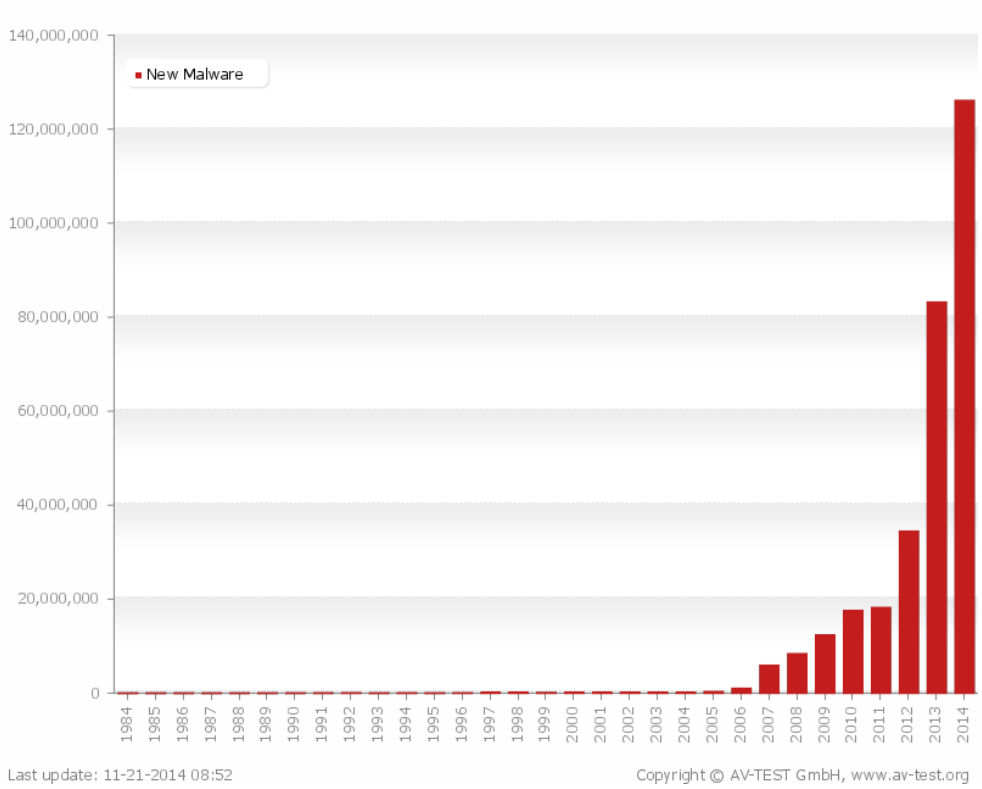
Število javnih servisov e-uprave strmo narašča

Smo ali nismo ogroženi?

Število internih servisov državne uprave strmo narašča

Smo ali nismo ogroženi?

Število varnostnih groženj v Internet svetu strmo narašča



Vir: www.av-test.org

Smo ali nismo ogroženi?

Državna omrežja so že po definiciji mamljiva za zlorabo

Smo ali nismo ogroženi?

- Informacijsko omrežje državnih organov je
  - Veliko
  - Geografsko razpršeno
  - Ne v celoti centralno kontrolirano

Torej grožnja je realna

- Ogroženost sodobnih informacijskih sistemov se strmo povečuje
- Državna omrežja so sama po sebi posebej mamljiva
- „Operaterska“ omrežja so težje kontrolirana, kot pa enovita centralizirana omrežja

Kaj pa je ogroženo?

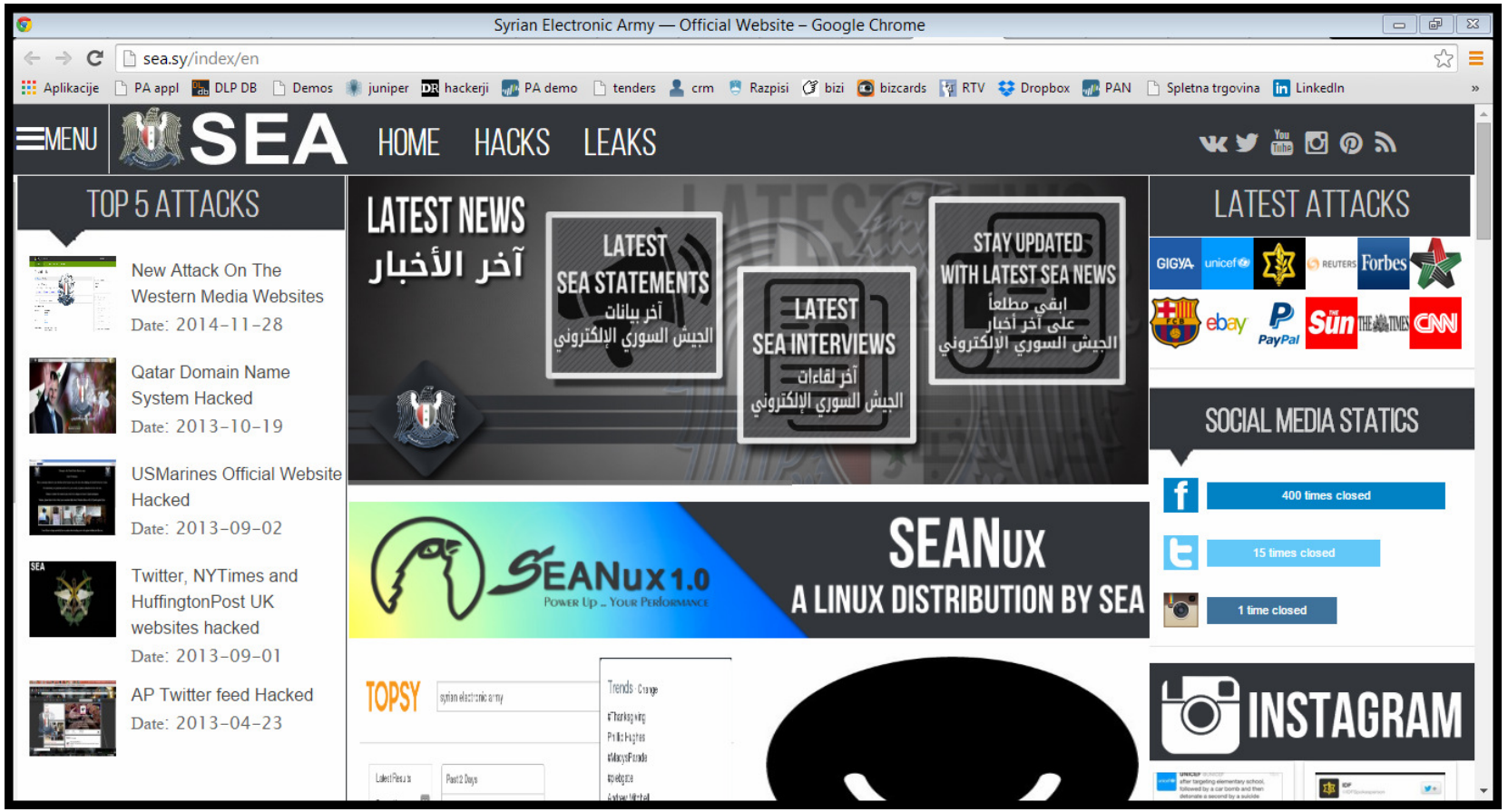
- Javni servisi državnih organov
- Osebni podatki državljanov
- Tajni podatki države
- Ugled države

Kdo pa nas ogroža?

Cult of Dead cow

Kdo pa nas ogroža?

Syrian Electonical army



Kdo pa nas ogroža?

PLA Unit 61398

Kdo pa nas ogroža?

Varnostno neosveščen uporabnik

Kdo pa nas ogroža?

Nezadovoljen ali kako drugače „slab“ pooblaščen uporabnik

Kdo nas torej ogroža?

- Naključni napadalci
- Usmerjeni napadalci
- Neosveščeni notranji uporabniki
- Zlonamerni pooblaščeni uporabniki

Aplikacije/servisi

- Informacijska varnost se je preselila na nivo aplikacije
  - Omrežje predstavlja zgolj osnovni nivo varnosti
  - Pomembna je varnost znotraj same aplikacije
    - Varnost pred zlorabami servisov
    - Varna identifikacija
    - Varnost pred nepooblaščenim dostopov do podatkov

Rešitve

- Zagotavljanje varnega okolja
  - Centralizacija in standardizacija arhitekture aplikacij
  - Centralizacija sistemskih virov
- Proaktivno varnostno preverjanje servisov in aplikacij
  - Varnostno preverjanje servisov pred zlorabami (penetration scan)
  - Varnostni pregled programske kode

Omrežje

- Omrežje zagotavlja
  - Osnovni nivo varnosti servisom in aplikacijam
  - Napredno varovanje omrežja pred naprednimi napadi
  - Centraliziran nadzor varnostnih dogodkov
  - Hitro ukrepanje ob sumih zlorab

Rešitve

- Uvedba **NG**varnostnih mehanizmov ob prihajajoči prenovi (NGFW, NG IPS, ipd.)
- Uvedba **SIEM** sistema – centralni nadzor varnostnih dogodkov
- Uvedba **APT** zaščit – zaščit pred naprednimi napadi
- Uvedba sistema za preprečevanje odtekanja podatkov - **DLP**
- Centralizacija in avtomatizacija varnostnih ukrepanj

Dvig varnostne inteligence

- Osveščanje/izobraževanje
- Upravljanje s tveganji
  - Kaj so sredstva?
  - Kaj so grožnje?
  - Kaj so posledice?
  - Kaj so ukrepi?

Kakšni so organizacijski izzivi?

Predpogoji za varno okolje

- Centralizacija upravljanja in nadzora skozi celotno omrežje
- Centralizacija storitev in aplikacij
  - Ni razpršenosti podatkov
  - Učinkovitejše zagotavljanje sistemske varnosti
  - Učinkovitejši nadzor nad varnostjo aplikacij

Kakšne so organizacijske rešitve?

Centralizacija varnostnih mehanizmov

- Centralno spremljanje in koreliranje varnostnih dogodkov
- Centralno uvajanje varnostnih pravil v omrežju in na aplikacijah
- Centralno preverjanje stanja varnosti na posameznih gradnikih
- Centraliziran odzivi na varnostne dogodke

Kakšne so organizacijske rešitve?

Centralizacija pravil

- Varnostna politika državnega omrežja (kaj se sme, kaj se ne sme)
- Delna centralizacija upravljanja s tveganji po ISO 27001 standardu
- Postopki in metodologija odziva na varnostne dogodke

Kakšne so organizacijske rešitve?

- Uvedba predpogojev za varno okolje s centralizacijo
- Centralizacija tehnoloških rešitev
- Centralizacija pravil

Kakšne so organizacijske rešitve?

Upeljava centralnega varnostnega telesa Gov-cert

Astec d. o. o.,
Stegne 31, Ljubljana
W: www.astec.si
E: info@astec.si
T: 01 200 83 00

Družini prijazno podjetje

?
?
?
?
?
?
?
?
?
?
?
?

astec