

Varnostne grožnje in tveganja v
informacijskih sistemih javne in državne
.....
uprave

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

astec

Smo ali nismo ogroženi?

Število javnih servisov e-uprave strmo narašča

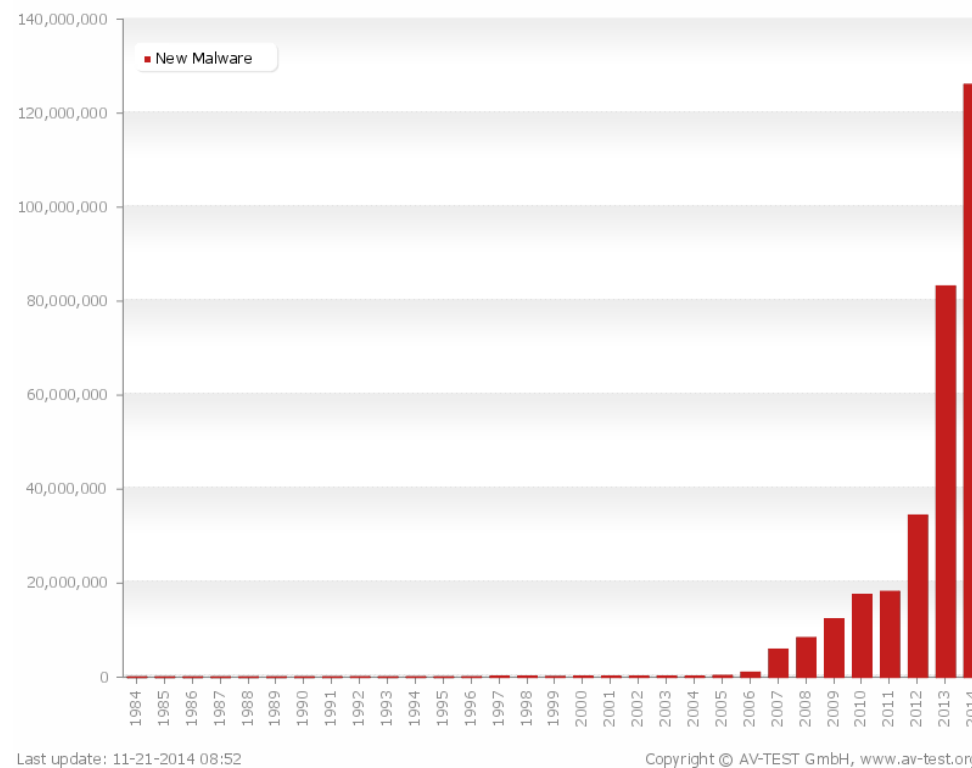


Smo ali nismo ogroženi?

Število internih servisov državne uprave strmo
narašča

Smo ali nismo ogroženi?

Število varnostnih groženj v Internetu 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
- „Operatorska“ 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

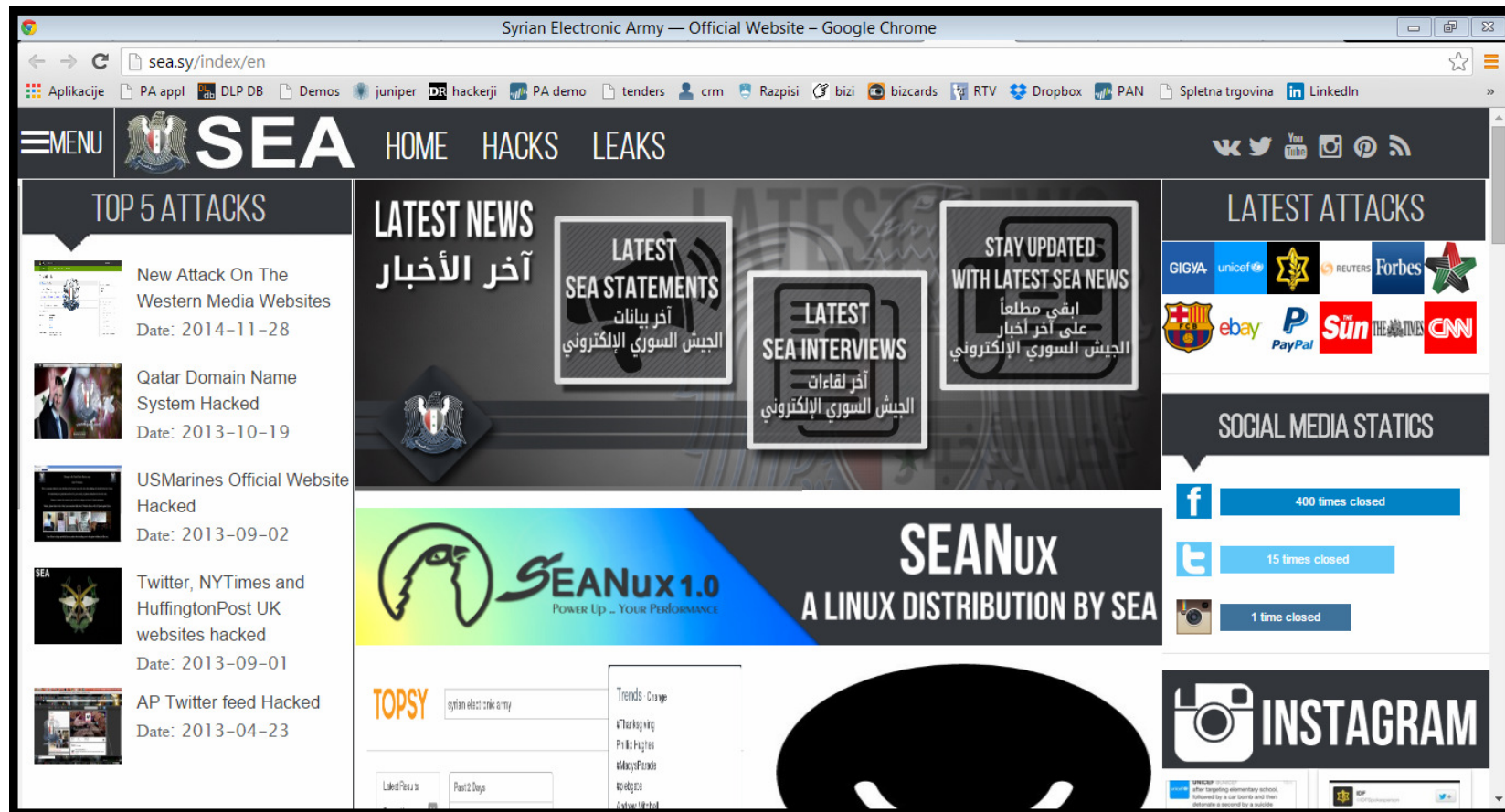
Kdo pa nas ogroža?

Cult of Dead cow



Kdo pa nas ogroža?

Syrian Electronical army



The screenshot shows the official website of the Syrian Electronic Army (SEA) in Google Chrome. The browser address bar displays 'sea.sy/index/en'. The website features a dark theme with a navigation bar at the top containing 'MENU', 'SEA', 'HOME', 'HACKS', and 'LEAKS'. Below the navigation bar, there are several sections:

- TOP 5 ATTACKS:** A list of recent attacks with dates:
 - New Attack On The Western Media Websites (Date: 2014-11-28)
 - Qatar Domain Name System Hacked (Date: 2013-10-19)
 - USMarines Official Website Hacked (Date: 2013-09-02)
 - Twitter, NYTimes and HuffingtonPost UK websites hacked (Date: 2013-09-01)
 - AP Twitter feed Hacked (Date: 2013-04-23)
- LATEST NEWS:** A section with headlines in Arabic, including 'آخر الأخبار', 'LATEST SEA STATEMENTS', and 'LATEST SEA INTERVIEWS'.
- LATEST ATTACKS:** A section displaying logos of various organizations and media outlets that have been targeted, including GIGYA, unicef, Reuters, Forbes, eBay, PayPal, Sun, and CNN.
- SOCIAL MEDIA STATICS:** A section showing the number of times social media accounts have been closed:
 - Facebook: 400 times closed
 - Twitter: 15 times closed
 - Instagram: 1 time closed
- SEANux 1.0:** A banner for 'SEANux 1.0 A LINUX DISTRIBUTION BY SEA' with the tagline 'POWER UP... YOUR PERFORMANCE'.
- TOPSY:** A section with a search bar and a list of trending topics.
- INSTAGRAM:** A section with an Instagram logo and a link to the SEA Instagram account.

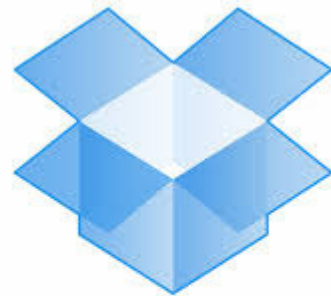
Kdo pa nas ogroža?

PLA Unit 61398



Kdo pa nas ogroža?

Varnostno neosveščen uporabnik



Dropbox



Kdo pa nas ogroža?

Nezadovoljen ali kako drugače „slab“ pooblaščen uporabnik

Are you ready to leave your job?



Kdo nas torej ogroža?

- Naključni napadalci
- Usmerjeni napadalci
- Neosveščeni notranji uporabniki
- Zlonamerni pooblašчени 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 dostopom do podatkov

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

- 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 systemske 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



?
?
?
?
?
?
?
?
?
?
?

astec