Dijagnoza sajber bolesti

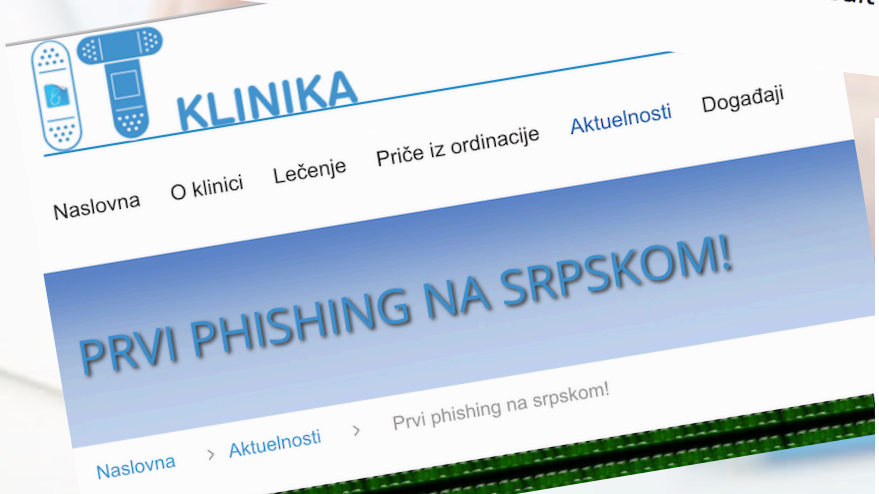
Vladimir Vučinić

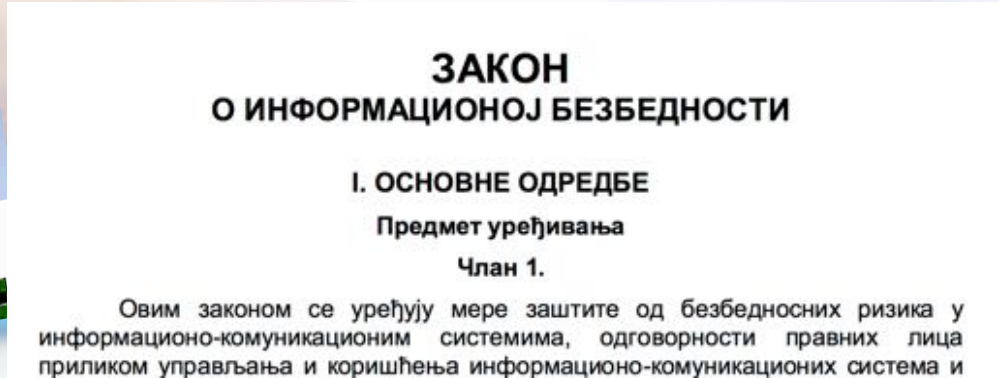
direktor

Net++ technology d.o.o.

Sajber zdravlje nacije

Serbia is also not immune to cyber threats. Last year, websites of official institutions and the media were victims of a direct distributed-denial-of-service (DDoS) attack in the aftermath of an incident at a football match with Albania. "Personal data of millions of citizens were leaked from the database of the Serbian Business Register Agency and e-mails of high-ranking interior ministry officials were taken over," said Vladimir Radunovic, Director of Cyber-security and E-diplomacy Programmes of Diplo Centre Civil Society Organization (CSO). According to Radunovic, a countrywide cyber attack could result in a direct loss of more than 10 million Euros per day.





ЗАКОН
О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

I. ОСНОВНЕ ОДРЕДБЕ

Предмет уређивања

Члан 1.

Овим законом се уређују мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и

Dijagnoza sajber bolesti

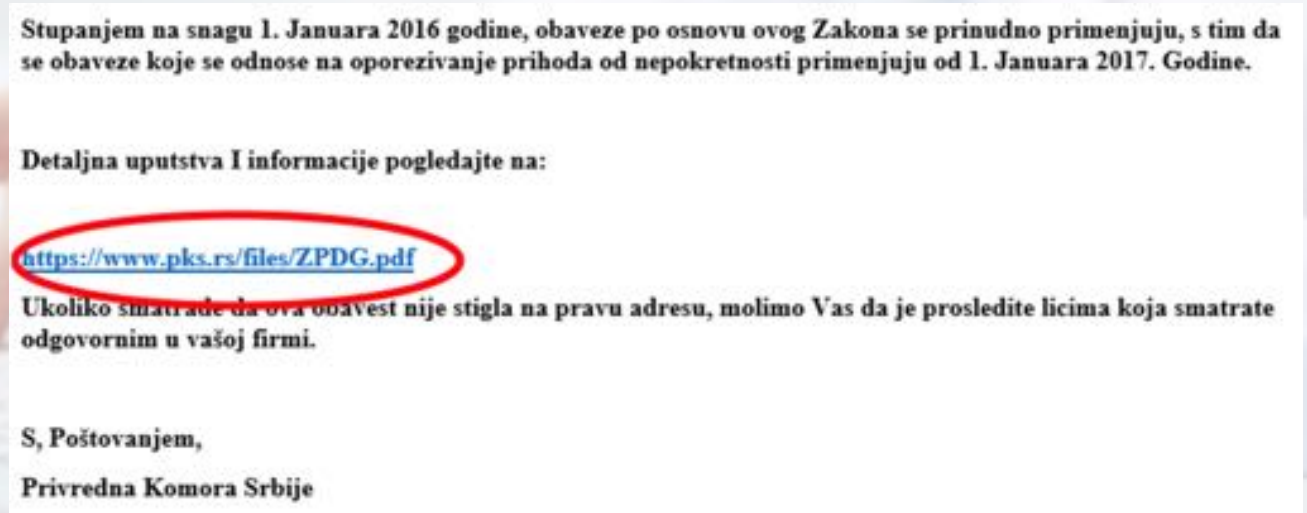
- Kasnimo za većinom zemalja, uključujući i okruženje (Zakon o informacionoj bezbednosti donet tek ove godine, nemamo CERT...)
- Slabo poznavanje i niska svest o IT sigurnosti (koliko ljudi klikne na račun T-mobile i sl.)
- Nedostatak ljudi u preduzećima koji bi se bavili isključivo IT bezbednošću
- Nedostatak sredstava
- ...

Lečenje

1. Prevencija – edukacija i podizanje svesti
2. Prevencija – sprečavanje pretnji pre nego što stignu do nas
3. Pravovremena dijagnoza – advanced threat protection
4. Lečenje – uklanjanje infekcije
5. Oporavak i jačanje imuniteta – sprečavanje ponovne infekcije i poboljšanje zaštite

1. Prevencija – edukacija i podizanje svesti

Kome je ovo poznato (možda je bolje pitanje: Kome nije)?



Stupanjem na snagu 1. Januara 2016 godine, obaveze po osnovu ovog Zakona se prinudno primenjuju, s tim da se obaveze koje se odnose na oporezivanje prihoda od nepokretnosti primenjuju od 1. Januara 2017. Godine.

Detaljna uputstva I informacije pogledajte na:

https://www.pks.rs/files/ZPDG.pdf

Ukoliko smatrate da ova obavest nije stigla na pravu adresu, molimo Vas da je prosledite licima koja smatrate odgovornim u vašoj firmi.

S, Poštovanjem,

Privredna Komora Srbije

Prvi phishing na srpskom

PC PRESS

Kompletna IT rešenja na jednom mestu

INTERNET · TELEFONIJA · CLOUD · HOSTING

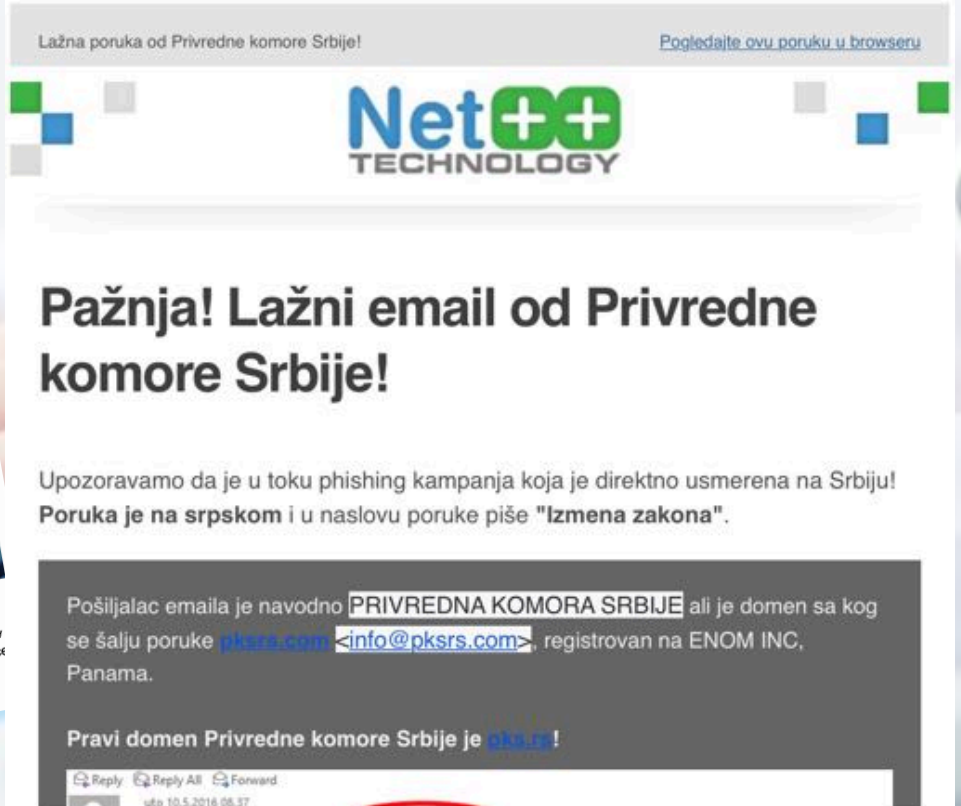
Vesti | Aktuelno | Softver | Hardver | Zabava | Internet | Bizit

Upozorenje: phishing na srpskom jeziku!

Na phishing smo odavno navikli (za neupućene, radi se o e-mail porukama koje imaju zaraženi prilog ili link koji vodi ka nekom zlonamernom kodu, sa 'ubedljivim' sadržajem i maskirane tako da se na prvi pogled ne primeti da se radi o prevari), ali smo takođe i naučili da je opasno otvarati poruke od nepoznatih pošiljaca, pogotovo na stranom jeziku, tako da ova vrsta pretnji u našim krajevima nije imala previše efekta

Ali, sada se pojavio phishing na srpskom jeziku, prilično dobro urađen, u obliku poruke navodno od Privredne komore Srbije, o navodnoji izmeni Zakona o porezu na dohodak građana, sa profesionalno napisanim tekstom, i u kojoj se poziva na preuzimanje navodnog PDF dokumenta. Ako dobijete takav e-mail, nipošto ne preuzimajte taj „PDF", jer se u stvari ne radi o PDF-u već o izvršnoj datoteci koja će napadaču omogućti kompletan daljinski pristup vašem računaru.

Detaljnije o ovom phishingu pročitajte na **sajtu IT Klinike**



Lažna poruka od Privredne komore Srbije! Pogledajte ovu poruku u browseru

Net++ TECHNOLOGY

Pažnja! Lažni email od Privredne komore Srbije!

Upozoravamo da je u toku phishing kampanja koja je direktno usmerena na Srbiju! **Poruka je na srpskom** i u naslovu poruke piše **"Izmena zakona"**.

Pošiljalac emaila je navodno PRIVREDNA KOMORA SRBIJE ali je domen sa kog se šalju poruke pksrs.com <info@pksrs.com>, registrovan na ENOM INC, Panama.

Pravi domen Privredne komore Srbije je pks.rs!

Reply Reply All Forward

uto 10.5.2016 08:37

KLINIKA

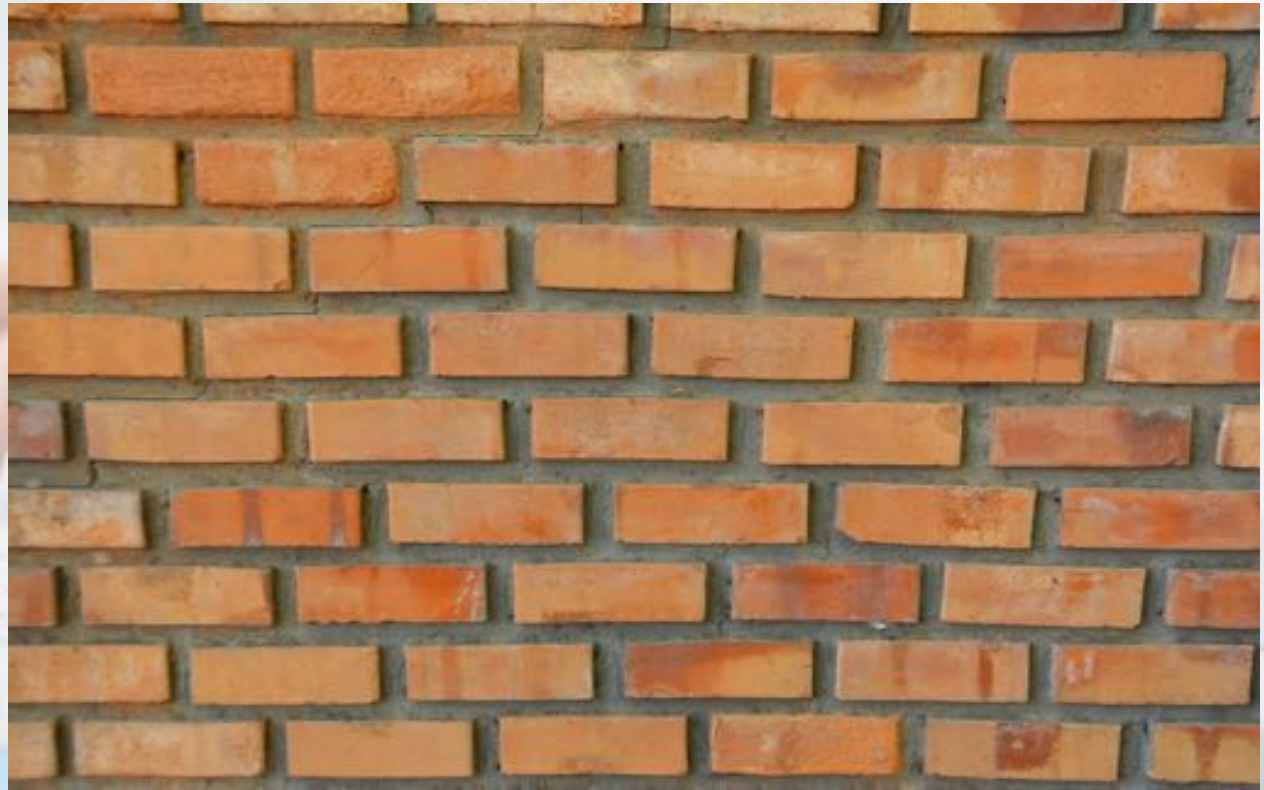
Prvi phishing na srpskom

- Veliki broj ljudi kliknuo i preuzeo .exe, startovao i instalirao virus (remote admin) – totalno nepripremljeni za “lokalizovan” phishing!
- Net++ technology prvi objavio i analizirao virus, poslao email, objavio i na www.it-klinika.rs
- U vreme slanja email-a samo jedan AV engine imao potpis i detektovao kao potencijalnu pretnju
- AV više nije dovoljan – sada je to jasno na ovom primeru
- Na desetinama računara u Srbiji primećena aktivnosti (konekcija spolja kod jednog IPS-a), tj. neko je pristupao računarima

1. Prevencija – edukacija i podizanje svesti – kako možemo da pomognemo?

- Net++ technology program podizanja svesti o IT bezbednosti za preduzeća (i za phishing) – obuka za zaposlene i za administratore
- Symantec Phishing Readiness
- Provera (test za zaposlene, prema potrebama)

2. Prevencija – sprečavanje pretnji pre nego što stignu



2. Prevencija – sprečavanje pretnji pre nego što stignu – kako možemo da pomognemo

- Next Generation Firewall (NGFW) – Palo Alto Networks, zato što klasičan firewall nije dovoljan!
- Symantec Messaging Gateway/Email Protect.cloud
- Net++ technology demo/test uređaji na raspolaganju
- Net++ technology instalacija/konfiguracija/podrška
- Net++ technology obuka administratora

3. Pravovremena dijagnoza – advanced threat protection

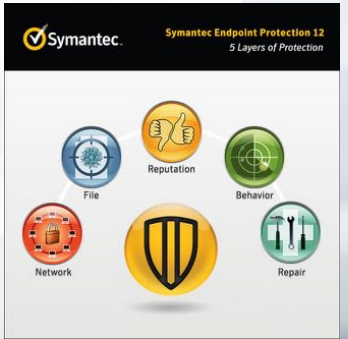
- Klasičan AV (antivirus) više nije dovoljan. Zašto? http://www.it-klinika.rs/price-ordinacija/analiza-virusa
- UTM uređaj više nije dovoljan. Zašto?
- Ciljani napadi su sve češći (izvor Symantec ISTR)
- Cyber kriminal je posao biznis!
- Krađa podataka se utvrdi tek nakon 3 ili više meseci (ISTR)

3. Pravovremena dijagnoza – advanced threat protection – kako možemo da pomognemo

- Symantec ATP
- Palo Alto Networks WildFire
- Net++ technology demo/test uređaji na raspolaganju
- Net++ technology instalacija/konfiguracija/podrška
- Net++ technology obuka administratora

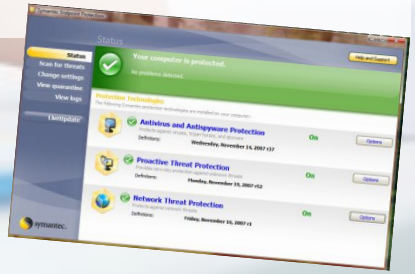
4. Lečenje – uklanjanje infekcije

- Pažljivo konfigurisanje AV
- Aktiviranje svih tehnologija zaštite na endpoint-u
- Stalno praćenje/nadgledanje sistema
- Neophodni kvalitetni alati za uporne pretnje
- Integracija sa ATP/APT sistemom zaštite
- Enkripcija
- Pažljivo konfigurisanje prava pristupa
- Backup!



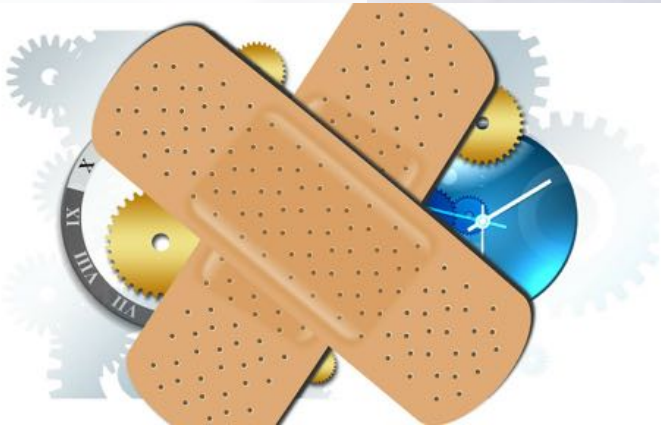
4. Lečenje – uklanjanje infekcije – kako možemo da pomognemo

- Symantec SEP/SEP.cloud/Encryption
- SymDiag/ručno uklanjanje
- Net++ technology demo licence na raspolaganju
- Net++ technology instalacija/konfiguracija/podrška
- Net++ technology health-check provera SEP-a
- Net++ technology obuka administratora



5. Oporavak i jačanje imuniteta – sprečavanje ponovne infekcije i poboljšanje zaštite

- Analiza postojećeg stanja i utvrđivanje koraka ka poboljšanju sistema IT bezbednosti
- Testiranje/PoC
- Plan poboljšanja, budžetiranje – procena troškova
- Konsultacije/saveti/iskustva
- Utvrđivanje KPI, praćenje



5. Oporavak i jačanje imuniteta – sprečavanje ponovne infekcije i poboljšanje zaštite – kako možemo da pomognemo

- SLA ugovor (podrška)
- Managed Security Services
- Analiza stanja/health-check
- Poboljšanje/zamena postojećih tehnologija zaštite
- Uvođenje novih tehnologija (NGFW, ATP…)
- Incident Response
- Edukacija

Hvala!

Vladimir Vučinić

vladimir@netpp.rs

(063) 245-250

Net++ technology d.o.o.