Digitalna bezbednost – Zaštita od Cyber napada

Armin Dinar – Direktor of Cybersecurity & IT Advisory Services

Jovan BogiĆeviĆ – Senior IT Consultant

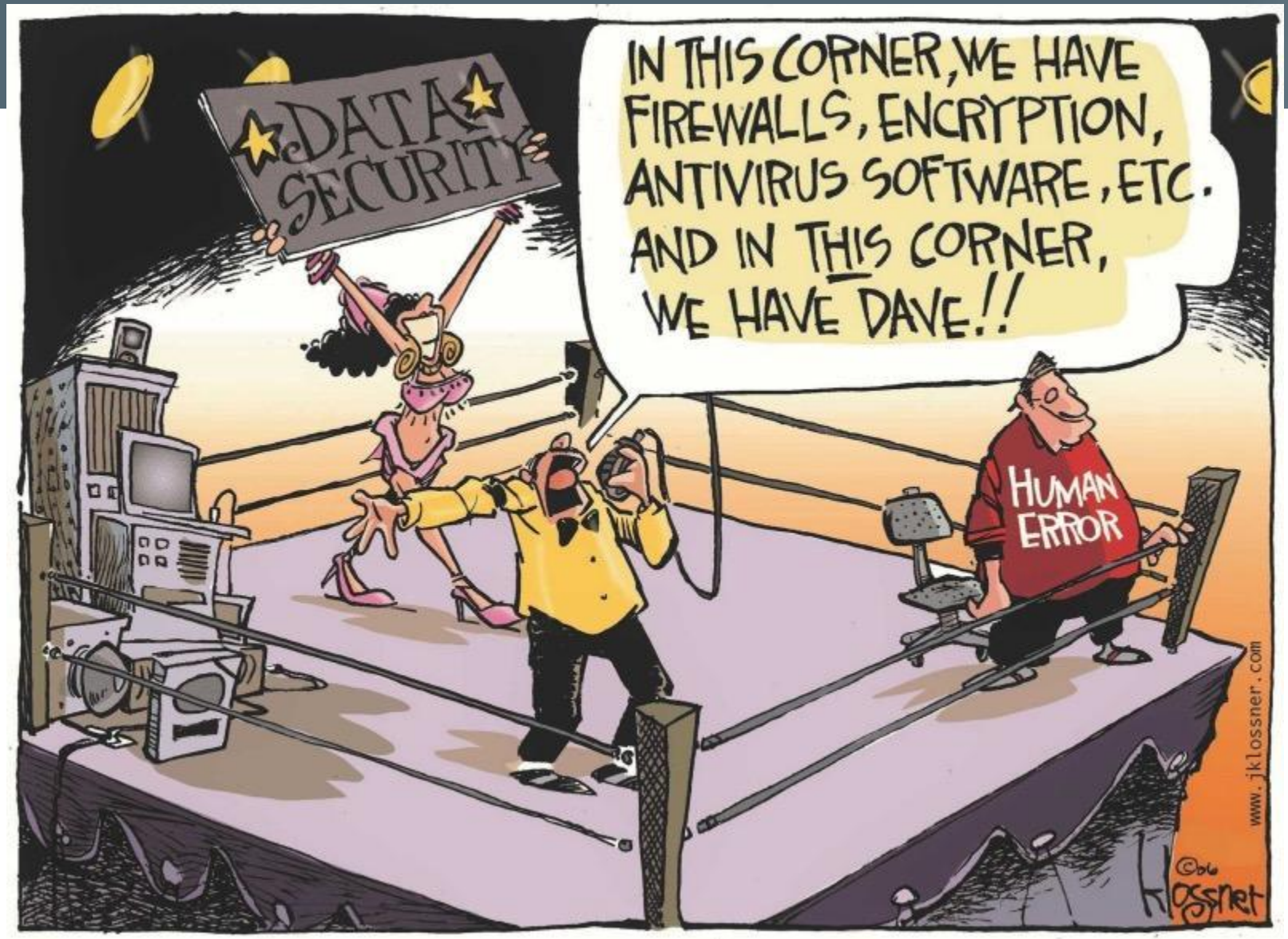
EY
Building a better working world

ANKETA

www.menti.com

Agenda

1. **Cyber bezbednosti**
2. Pristupi zaštiti od Cyber napada
3. Social engineering – pokazne veŽbe


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner

Svest od Cyber napada u Svetu

Japan je pokrenuo nacionalnu kampanju svesti o informacionoj bezbednosti u susret Olimpijskih igara 2020. godine.

Etičkim hakovanjem građana i adresiranjem njihovih ranjivosti oni žele pojačati bezbednost uređaja i svest na ovu temu. U okviru kampanje biće obuhvaćeno preko 200 miliona uređaja.

Source: https://www.weforum.org/videos/archive/

Definicije rizika primećene kroz industrije koje možete susresti

Operativni rizik je rizik gubitaka koji nastaju zbog neadekvatnih procedura i neuspelih internih procesa, ljudskog faktora, sistemskih ili eksternih događaja.

Tehnološki Rizik

Tehnološki rizik predstavlja podkategoriju Operativnog rizika i odnosi se na potencijalni negativni ishod, štetu, gubitak, neuspeh ili prekid koji proizilazi iz upotrebe i oslanjanja na računarski hardver, softver, uređaje, sisteme, aplikacije i mreže.

Informaciona bezbednost

Odnosi se na rizike koji utiču na poverljivost, integritet i/ili dostupnost informacija. Te informacije mogu biti u digitalnom formatu (u okviru Tehnološkog rizika) ili u fizičkom formatu (van okvira Tehnološkog rizika).

Cyber Rizik

Cyber rizik je deo Tehnološkog rizika i informacione bezebednost. Odnosi se na rizike koji su počinjeni od strane zlonamernog aktera preko digitalnih komunikacionih kanala, sa ciljem distribucije, izmene ili ometanja digitalne imovine organizacije.

Note:

EY-a definicija „cyber sigurnosti“ i „informacione bezbednosti“ je ista. Međutim, neke organizacije još uvek smatraju da je sajber sigurnost uži pojam u okviru informacione bezbednosti. Na ovom slajdu su prikazane definicije kompanija, nad kojima je vršeno istraživanje.

ANKETA

Da li vaša organizacija sprovodi procenu IT rizika koja obuhvata i cyber rizik?

Motivi cyber napada i njihov globalni rast

Cyber napad u najširem smislu, znači napad na neki kompjuterski servis sa ciljem da se korisnicima onemogući njegovo korišćenje, preuzme kontrola ili preuzmu podaci. Iako ima mnogo varijanti napada, čak više od 15, ovaj pojam najčešće čujemo u kontekstu napada na neku web stranicu tj. javno dostupne servise neke organizacije.

Dok su neki tipovi cyber pretnji prisutni već godinama, ulaskom u 2019. mnogi postaju kompleksniji ili menjaju dizajn. Rizik raste posebno kako se organizacije premeštaju svoje procese u raznovrsna i hybrid - cloud okruženja.

Motivi

1	Politički
2	Izazov
3	Sabotaža
4	Konkurentnost
5	Finansijski
6	Društveni

1 IoT cyber napadi su porasli 600 procenata samo u 2017. godini. Internet of Things je doveo do širenja mrežnog sloja sa velikim brojem krajnjih tačaka, što olakšava napadaču da ugrozi mrežu. Maliciozni napadači mogu iskoristiti IoT uredjaje i mobilne uredjaje da oforme botnets ili pokrenu DDos napade.

2 Cloud napadi – Microsoft je izveštavao da se u 2017. godini broj „cloud-based“napada povećao za 300 procenata. Potrebno je zaštititi se od „cloud-based“ napada implementacijom rešenja novijih generacija dizajniranih za cloud s obzirom da se nije moguće zaštititi menjanjem svrhe tradicionalnih sigurnostnih alata namenjenih zaštiti „on premise“ rešenja.

Ransomware - Barkley Team je procenio da će ransomware prouzrokovati troškove biznisu u iznosu od 11.5 milijardi dolara u 2019. godini. Ransomware je jedan od najopasnijih napada s obzirom da preuzima i enkriptuje podatke zahtevajući otkup za povrat podataka. Kripto valute su načinile ransomware napade efektivnijim, s obzirom da najčešće nije moguće ući u trag transakcijama.

3 Phishing - Iako je prisutan već dugo i dalje je u porastu ovaj tip napada (65% u 2017.). Društveni inžinjering je i dalje jedan od najtežih napada za zaštitu s obzirom da je okrenut ljudima. Phishing napadi mogu dovesti do krađe kredencijala što može dovesti do kradje podataka.

4

Cyber bezbednost i digitalna transformacija

Izazovi

87%

Članova izvršnog odbora nemaju dovoljno poverenja u cyber bezbednost svojih organizacija navodeći agilnost kao ključni izazov

1. Cyber bezbednost i digitalna transformacija su ključne mnogim biznisima, ali često nisu usaglašene

2. Organizacija moraju usaglasiti ove konvergirati ove 2 funkcije u procesu pronalaženja održive i uspešne inovacije

3. Uključivanje cyber bezbednosti u proces digitalne transformacije može biti „business enabler“ pre nego element usporavanja procesa

Transformacija Cyber bezbednosti

Svaki biznis koji je povezan na internet je meta cyber napada.

Cyber napadači postaju sve više sofisticirani, koriste napredne „phishing“ i malware tehnike kako bi našli slabe tačke u organizacijama.

Servisi transformacije cyber bezbednosti pomažu kompanijama da reše mnoge sigurnosne izazove sa kojima se suočavaju na dnevnom nivou, i da razviju efektivna rešenja koristeći ljude, procese i tehnologiju – čime bi omogućili bolje sigurnosne i rizične odluke, smanjili troškove koji se odnose na upravljanje sigurnosnim rizicima, i poboljšali svoj nivo informacione sigurnosti. Trenutno se nalazimo u novom talasu cyber bezbednosti koji zahteva od organizacija da razmišljaju na koji način će alocirati svoje resurse.

Global Information Security Survey'18

- 87% posto ispitanika je odgovorilo da im je potrebno 50% ili veće povećanje budžeta za cyber bezbednost.
- 36% Članova odbora ima dovoljno znanja o cyber bezbednosti kako bi efikasno nadgledali cyber rizike.
- 89% ispitanika je izjavilo da funkcija cyber bezbednosti ne ispunjava u potpunosti ciljeve organizacije.
- 12% ispitanika misli da je velika šansa da bi primetili sofisticirani cyber napad
- 63% organizacija i dalje sprovodi izveštavanje o cyber bezbednosti samo unutar IT funckije
- 57% organizacija nema, ili imaju neformalan „threat intaligence“ program

ANKETA

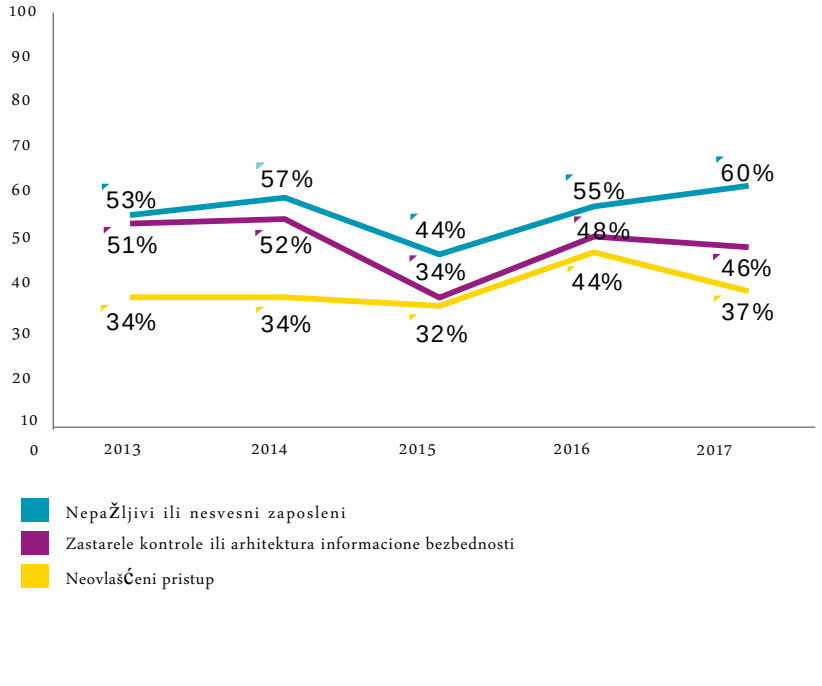
Da li je vaš budžet za tople napitke (kafu) veći od vašeg budžeta za cyber?

Kako se orijentacija promenila tokom godina?

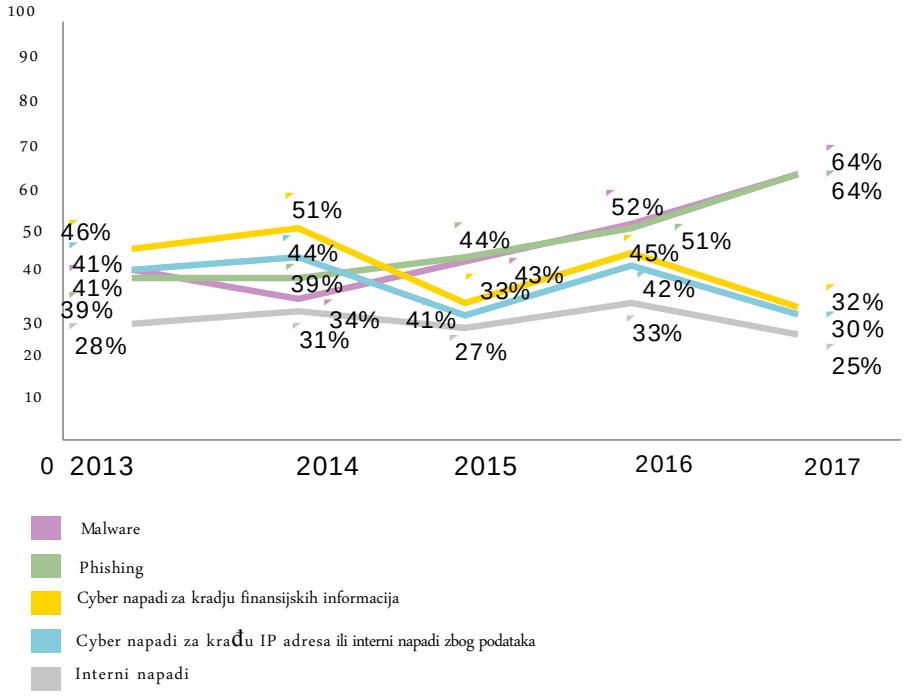
Organizacije se najčešće suočavaju sa raznim napadačima. Odgovor na napade mora biti na više nivoa sa fokusom na najčešće napade.

Pored toga organizacije moraju pripremiti i detaljniji plan odbrane kako bi se odbranili od naprednijih napada.

Ranjivosti



Pretnje



S obzirom da je neizbežno da će neki od napada uspešno proći sve linije odbrane potrebno je fokusirati se i na to koliko brzo je moguće uočiti napade kao i koliko efektivno možemo ukloniti posledice.

Source: EY Global inforamtion security survey

Agenda

1. Cyber bezbednost
2. **Pristupi zaštiti od Cyber napada**
3. Social engineering – pokazne veŽbe

Digitalna bezbednost – Benchmark pristup

Faze analize cyber pretnji i odbrana od napada

Kako bi organizacija bila spremna za odbranu od cyber napada potrebno je proceniti organizaciju kroz 5 faza prema predloŽenom pristupu za Informacionu bezbednost.

PredloŽen pristup odbrane od cyber napada se zasniva na dvostrukoj analizi – „Od vrha ka dnu“ i „od dna ka vrhu“

Benchmark pristup

Faze	FAZA 1		FAZA 2		FAZA 3		FAZA 4		FAZA 5
Oblast	Mapiranje mreŽe	1	Cyber threat management	2	Social engineering	3	Security Configuration Review	4	Cyber Risk management

Cyber threat management
Analiza ranjivosti i penetraciono testiranje

1 **Reconnaissance – Izviđanje**

Prva faza obuhvata sakupljanje relevantnih informacija o sistemu (kako sistem funkcioniše i potencijalne ranjivosti). U ovoj fazi se definiše obim i cilj testiranja kao i metodologije testiranja koje će se koristiti.

2 **Scanning – Skeniranje**

Sledeći korak je razumevanje ciljne aplikacije, kako „odgovara“ na razne napade. Skeniranje se radi statičkom i dinamičkom analizom.

3 **Gaining Access – Dobijanje pristupa**

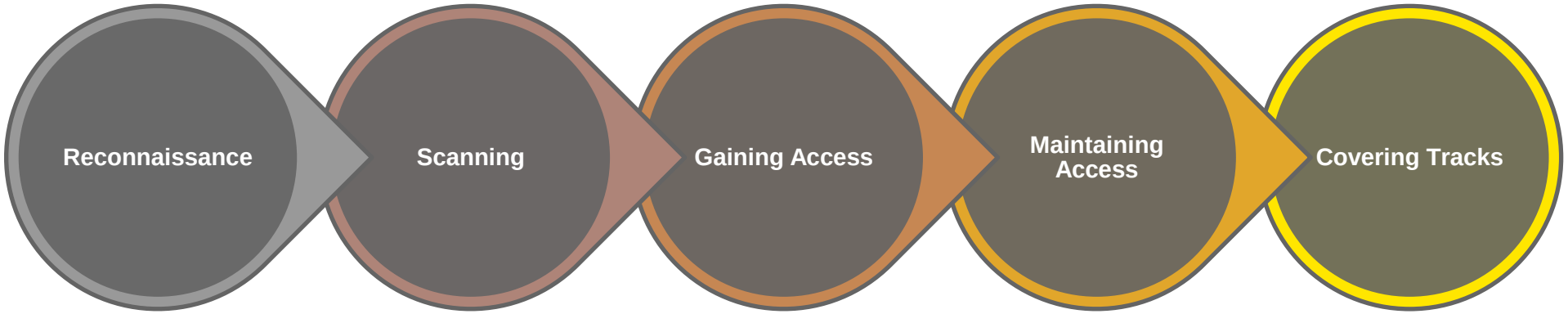
Dobijanjem pristupa korišćenjem znanja prikupljenog tokom prethodne 2 faze omogućava napadaču da eksploatiše ciljni sistem i otkrije ranjivosti sistema.

4 **Maintaining Access – zadržati pristup**

U ovoj fazi cilj je ostati konstantno u ciljanom sistemu kako bi se prikupilo što više informacija o sistemu. Cilj ove faze je da se simuliraju napredne pretnje koje ostaju u sistemu nedetektovane mesecima i preuzima osetljive podatke o organizaciji.

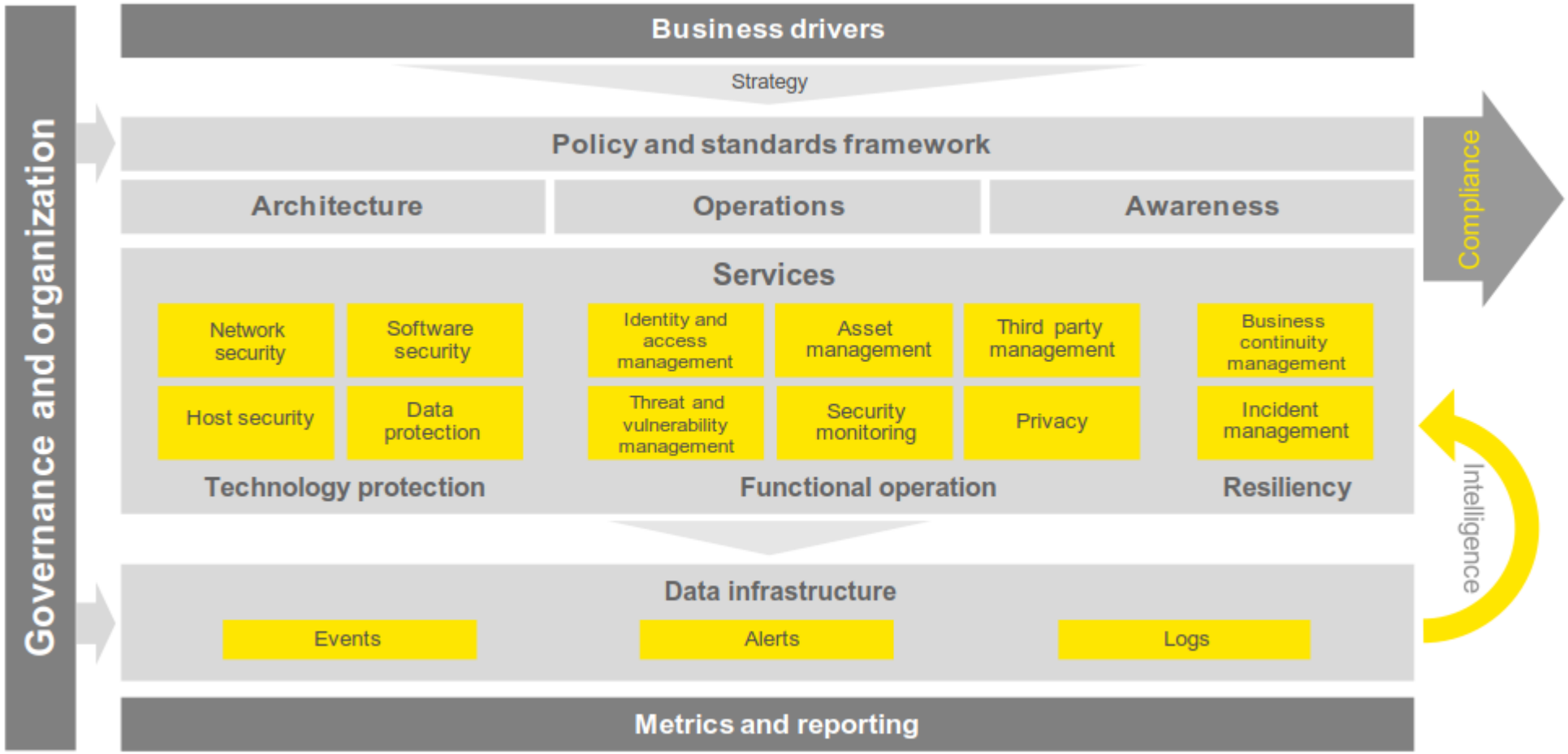
Covering Tracks– Prikrivanje tragova

5 Ovo je finalna faza prikrivanja tragova napada i prikaz svih rezultata penetracionog testiranja. Izveštaj prikazuje i sve ranjivosti sistema, podatke kojima je pristupljeno i koji su oštećeni prilikom napada kao i vreme koje je potrebno napadaču da ostane u sistemu neotkriven.



Cyber Risk Management
Domeni informacione bezbednosti

Identifikovali smo ključne domene u našem okviru Informacione bezbednosti koji su adresirani.

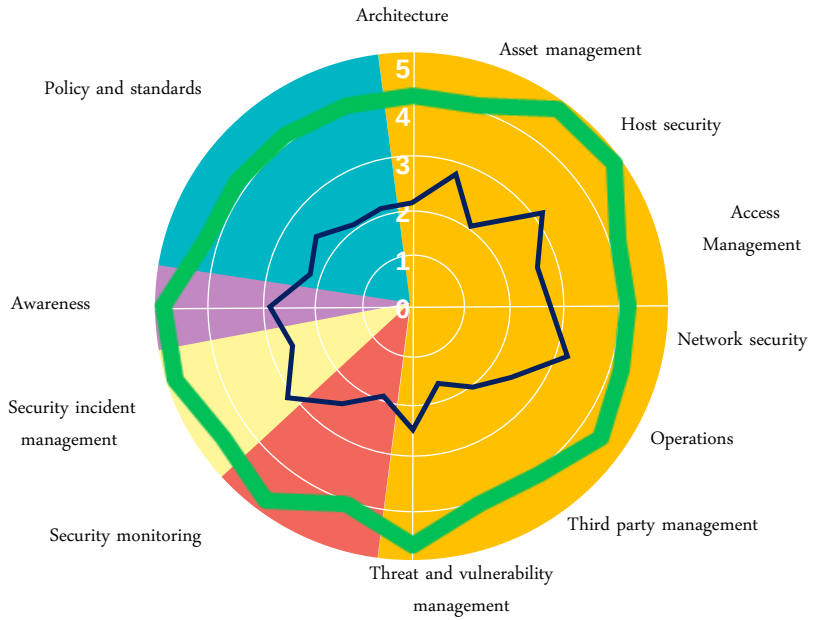


Cyber Risk Management
Cyber program management alat

CPM Alat je dizajniran za analizu i preporuke koje mogu pomeriti organizaciju sa trenutnog stanja na Željenu spremnost za cyber napade. Istovremeno, oprema organizaciju kako bi se ograničila izloženost nepredvidivim cyber napadima.

- Cyber program management alat pomaže organizaciji da:
  - Razume rizik izloženosti organizacije
  - Proceni nivo zrelosti trenutnog programa Informacione bezbednosti i identifikuje ključne oblasti za unapredjenje
  - Napravi i prioritizuje mapu za ulaganje u projekte i inicijative organizacione promene
  - Sakupi informacije i uporednu analizu sa drugim organizacijama
  - Potvrdi da su ulaganja u sigurnost poboljšala stanje i poziciju informacione bezbednosti

CPM Spider Web



Cyber Risk Management

Cyber program management alat – Rezultati CS programa za reprezentativne klijente

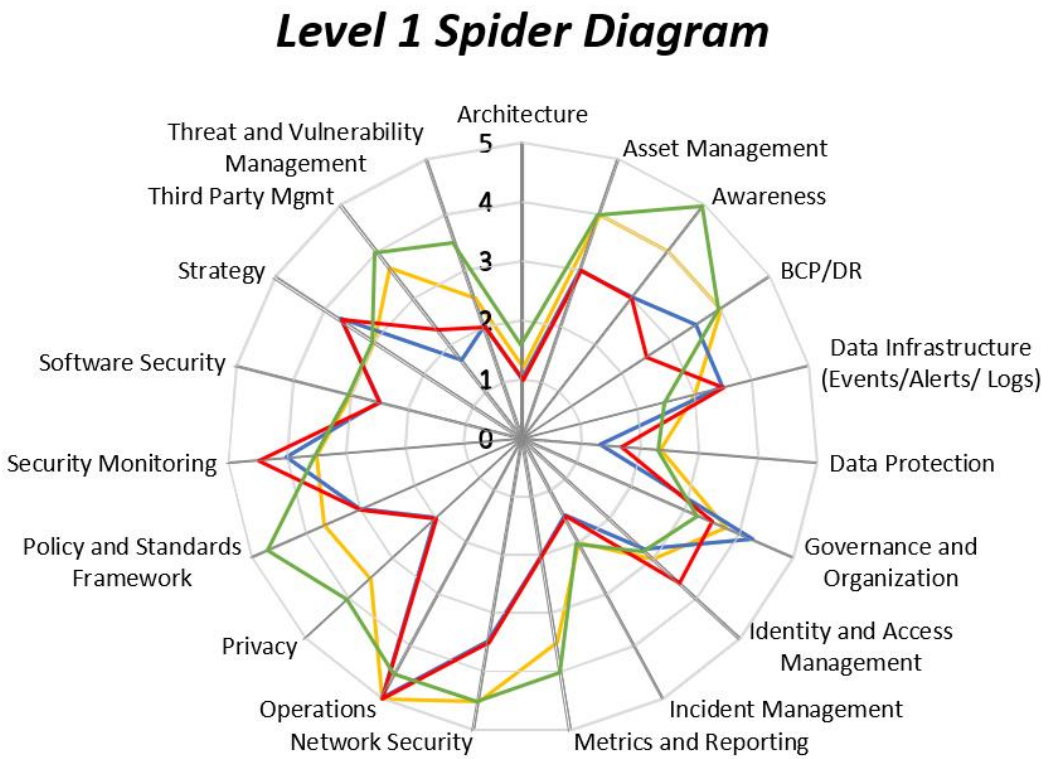
Primer kriterijuma za oblasti

- Da li postoji uspostavljen tim za odgovor na incidente?
- Kako organizacija vrši klasifikaciju podataka?
- Opisati pristup organizacije za „ threat and vulnerability management“ uključujući ključne role i odgovornosti.
- Kako je bezbednost integrisana u SDLC?

Najniže rangirane oblasti

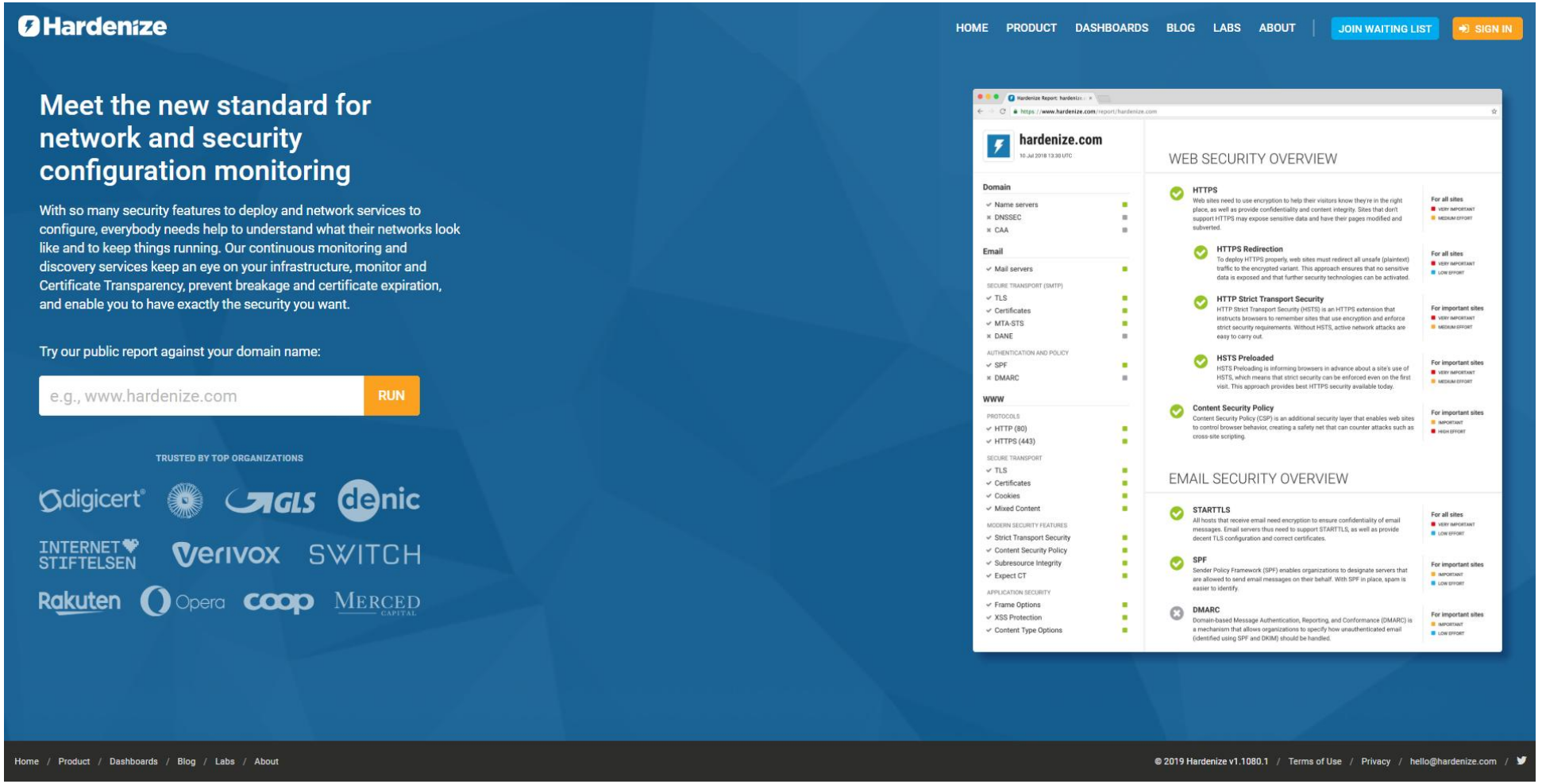
Domain	Average score
Architecture	1.20 – Low ranking
Incident Management	1.75 – Low ranking
Data Protection	1.92 – Low ranking
Threat and Vulnerability Management	2.50 – Medium ranking
Software Security	2.75 – Medium ranking

CPM Spider Web



Analiza host-a web sajta, mreže i sigurnosne konfiguracije

- Hardenize predstavlja alat koji omogućava sveobuhvatnu i besplatnu analizu web sajta i sigurnosne konfiguracije (“high level”)



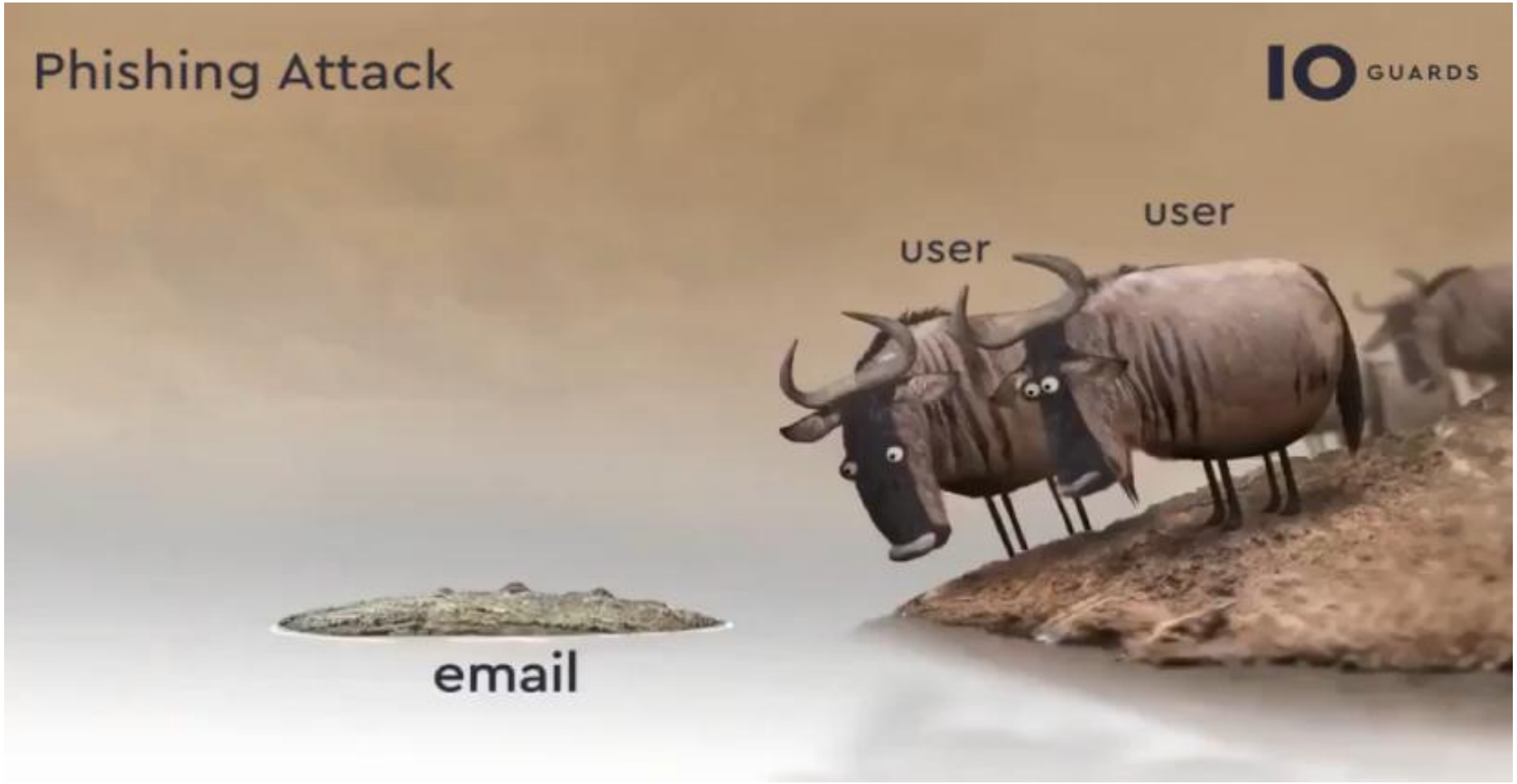
Agenda

1. Cyber bezbednost
2. Pristupi zaštiti od Cyber napada
3. **Social engineering – pokazne veŽbe**

Social engineering

“Phishing” napadi

- Ljudi su uvek bili najslabija karika u lancu zaštite. „Phishing“ i društveni inŽenjering obuhvataju 93 procenata svih prodora u sisteme (Verizon 2018. Izveštaj istraga o curenju podataka 2018.)
- Uz odgovarajuĆi trening i kampanje podizanja svesti kod zaposlenih o cyber napadima moguĆe je pripremiti zaposlene na ovakve napade.



Source: https://10guards.com/en/#main

Primer 1 - Virustotal

- Alat za analizu potencijalno malicioznih dokumenata
- Alat za analizu I proveru potencijalno malicioznih URL-ova I detekciju malware-a

VIRUSTOTAL

Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE | URL | SEARCH

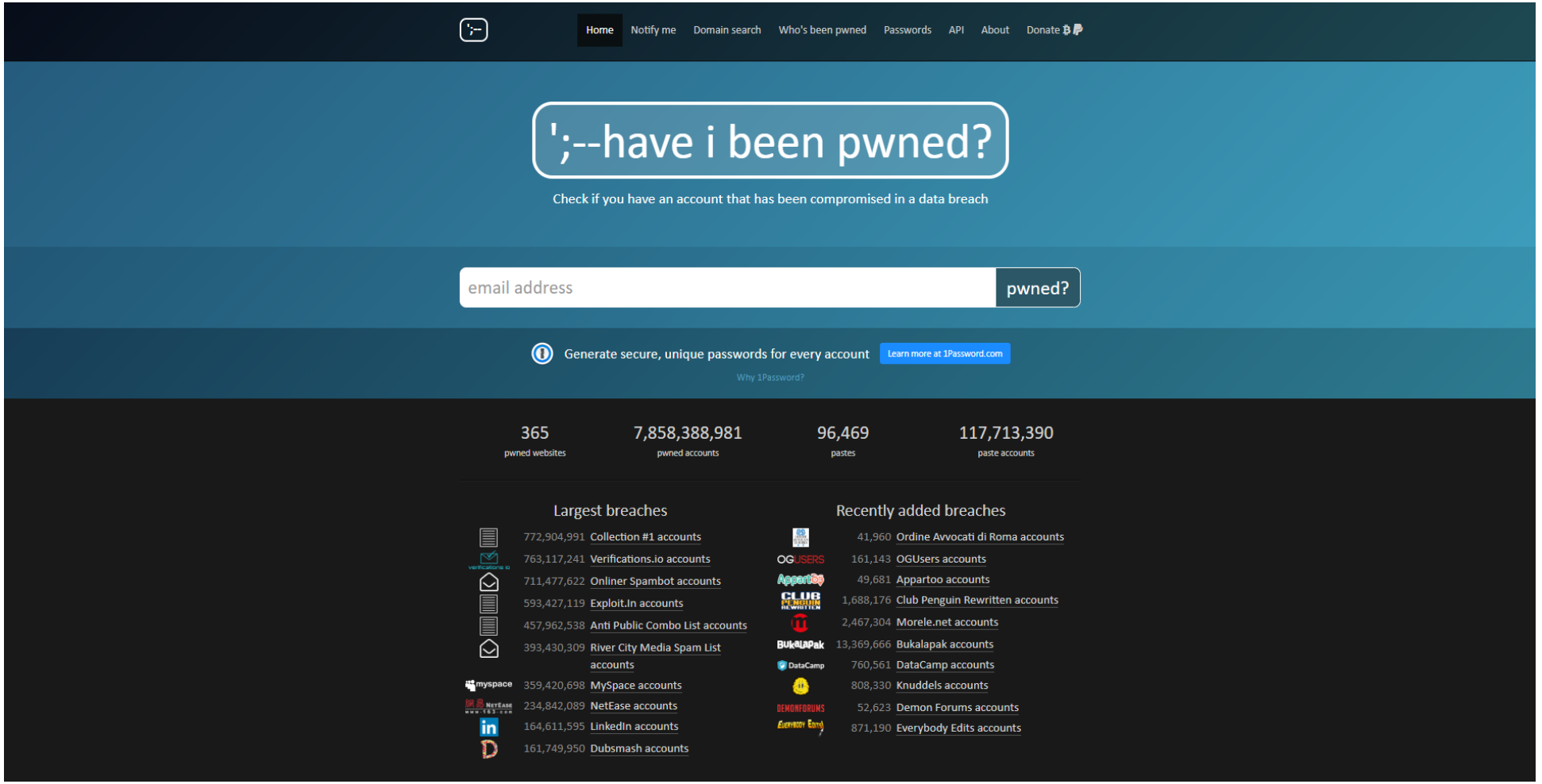
Search or scan a URL

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our Terms of Service and Privacy Policy. Learn more.

Source: www.virustotal.com

Primer 2 – ihavebeenpwned.com

- Alat za proveru ukradenih kredencijala u najvećim poznatim „data breachevima“



Source: www.ihavebeenpwned.com

EY

Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal N26. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

www.ey.com/cs/en/home

© 2019 Ernst & Young AB, All Rights Reserved.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.