Izkušnja izvajanja programa varnostnega osveščanja uporabnikov ter komuniciranja z deležniki med varnostnim incidentom

dr. Izidor Golob, CISA, CISM, ITIL F
Univerza v Mariboru

Nekaj o UM, organizaciji in uporabnikih

- ~2500 zaposlenih, ~1000 zunanjih sodelavcev, ~20.000 študentov
- skupne poslovne funkcije uporabljajo skupno programsko opremo
  - enotna uporabniška izkušnja
  - možen stroškovno učinkovit sistem upravljanja in podpore
- že 10+ let v uporabi rigorozen sistem upravljanja identitet
  - prehod je trajal cca. 5 let
- Informacijska varnostna politika sprejeta 2013, od takrat tudi redna izobraževanja
- Varnostni incidenti so dnevna praksa
  - nujna je triaža
  - izkušnje sodelovanja s policijo, IVP, SI-CERT, …
- nismo NIS-2 zavezanci

I. VARNOSTNO OSVEŠČANJE

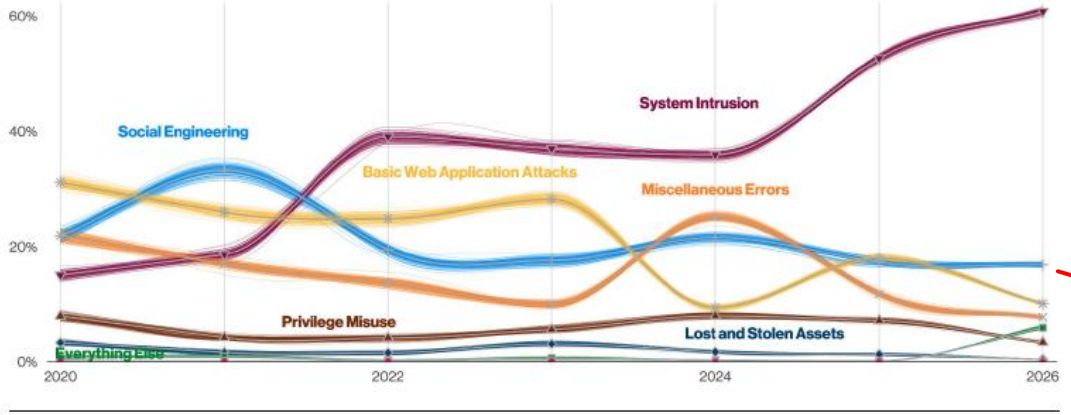
Varnostno osveščanje

- Izobraževanja so najmanj dvakrat letno, pri čemer:
  - gre za kombinacijo izobraževanj na daljavo in v predavalnici
  - vključujejo tipična področja od fizične varnosti naprej
  - izobraževanja niso obvezna
  - pogosto gre za razlago določil informacijske varnostne politike
- že leta 2017 smo bili naročniki platforme za phishing, kasneje opuščeno (nejasna učinkovitost / uspešnost, stroški)
- pomanjkanje (namenskega) osebja za zagotavljanje informacijske varnosti in osveščanja je težava, ampak…

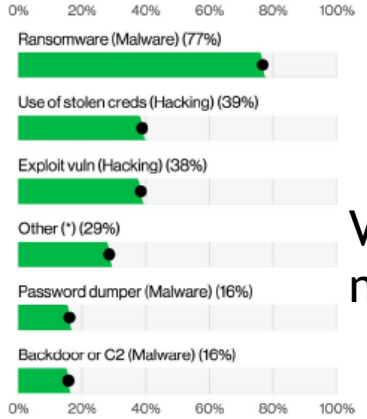
Naše izkušnje:

- uporabniški del:
  - izrazito izstopa elektronska pošta
    - porast vključevanja uporabnikov po vpeljavi SPF, DKIM, DMARC mehanizmov 2016
    - praktično nemogoče lastno upravljanje: kompromis *varnost proti prikladnost*
- večja phishing simulacija leta 2024: manj kot 3 % „ujetih“
- tudi 3 % (n= ~ 70) je veliko (preveč!?), poskušali smo razumeti obnašanje uporabnikov:
  - „Zavedal sem se, da je bilo nekaj sumljivo, vendar sem vseeno kliknil.“
  - „Na mobilnem telefonu mi informacije o domeni pošiljatelja ni pokazalo.“
  - „Ne razumem, kaj od mene želite. Nisem tehnično podkovana oseba.“
  - „Mudilo se mi je in nisem imel časa preveriti.“

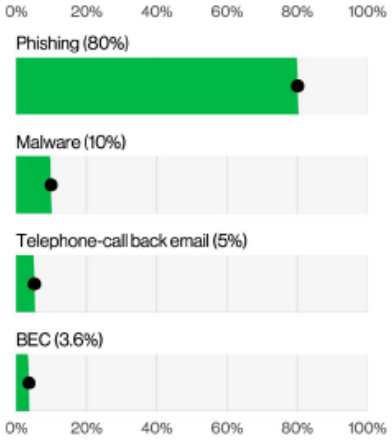
Verizon 2026 Data Breach (20. 5. 2026)



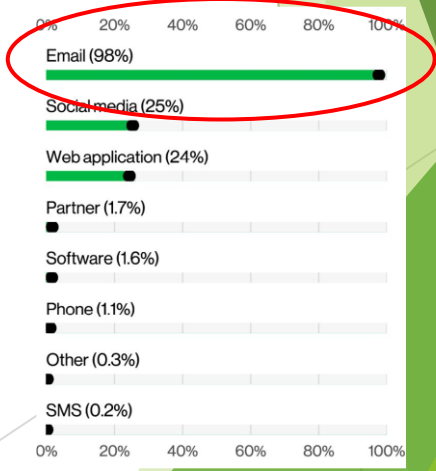
Klasifikacijski vzorci napadov



Vdor v sistem:
najpogostejše vrste



Delež tipov napak preko e-pošte (n=3.709.045.972)



Vektorji napada pri socialnem inženiringu

Mesečno poročilo o e-elektronski pošti za UM

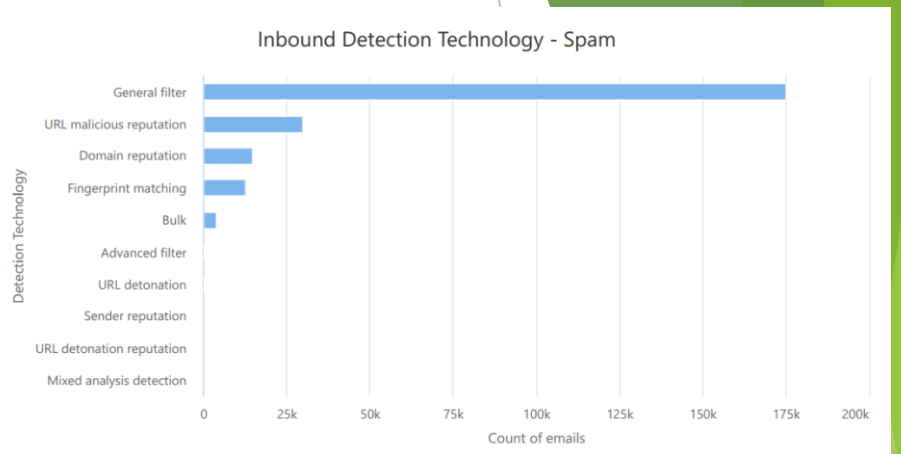
1.146.153
Total Messages

15.214
Protected

0
Partially Protected

0
Unprotected Recipients

100.0%
Coverage



54.325
Phishing Threats Identified

769
Malware Threats Identified

236.129
Spam Messages Identified

99.65%
Malicious Catch Rate

17.024
Messages Quarantined

144
Messages Released

0.8%
Release Rate

147
AI Detected Phish Messages

137
Contact Establishment Phish Messages

70
AI Detected Malware Messages

70
Malware Downloader Attachments

622
Detonations detecting phish threats

2
Detonations detecting malware threats

Naše izkušnje – nadaljevanje:

- pri izobraževanju je boljša razdelitev na različne skupine uporabnikov
- „Ne!“ igrifikaciji: nezdravo tekmovanje (lov za metriko), ne odgovarjajo vsi itd.
- Če bi bili vsi „osveščeni“, bi podpora pregorela
  - Tipični uporabnik ne razume niti kaj je glava sporočila
- zaostajanje nad vedno novimi grožnjami
  - maj 2026: YellowKey BitLocker Bypass, Kali 365, AI (Mytos): „Seveda ti lahko pomagam pripraviti malware!“.
- Saj ni res, pa je: najeti vsiljivci so bili postreženi s kavo

Ali je res vse zaman in bomo obupali?

- Splošne, enostavne metrike za uspešnost izobraževanja danes več ne zadoščajo
- Phishing testi so diagnostika, ne pa neposredna meritev zmanjšanja tveganja
- Zavedanje (poznavanje tveganj) ni enako dejanski spremembi obnašanja
  - za „tipičnega uporabnika“ je hitrost sprememb (nova tveganja) enostavno prevelika
  - potrebne so tehnike uvajanja sprememb: uvajanje PAM je trd oreh!
- vedno novi in novi scenariji, velika kompleksnost zmanjšuje čas in uspešnost reševanja

II. KOMUNIKACIJA NA PRIMERU VARNOSTNEGA INCIDENTA

KRONOLOGIJA VARNOSTNEGA INCIDENTA

- Začetek 24. 10. 2024 ob 20.03h, potrditev 25. 10 ob 2.45h
- preventivno obveščanje IVP, SI-CERT ob sumu, 23.00h
- sestanek ožje skupine ob 4.00h
- obveščanje vodstva ob 4.52h
- prvi sestanek krizne skupine ob 8h (10+ ljudi)
- kasneje vzpostavljen „war-room“ (7-21h)

KOMUNIKACIJA V ČASU VARNOSTNEGA INCIDENTA

- Prepoved (omejitev) komunikacije članov ožje skupine
- **Interna komunikacija:**
  - Vodstvo
  - Vodje poslovnih procesov: vzpostavitev alternativnega izvajanja
  - zaposleni, študenti
- **Zunanja komunikacija:**
  - novinarji
  - policija
  - Informacijski varnostni pooblaščenec
  - SI-CERT
  - drugi (slo-tech)
- skupnost je pokazala veliko mero razumevanja
- težava je bil tudi kanal obveščanja
- prioriteta št. 1: izplačilo plač – s strani vodstva postavljena kot prva prioriteta

Prejeta vprašanja:

- Kaj se je zgodilo?
- Kateri sistemi in podatki so prizadeti?
- Kakšen je vpliv (študenti, zaposleni, zunanji)?
- Ali so bili prizadeti osebni podatki?
- Ali so bili obveščeni regulatorji, policija, SI-CERT?
- Ali bodo prizadeti obveščeni: kaj in kako?
- Ali je napadalec identificiran? **Ali ste res plačali 10 MIO EUR odkupnine?**
- Kdaj bodo sistemi spet vzpostavljeni?
- Kakšne so finančne in druge posledice?
- Kdo je odgovoren?
- Kakšni so stroški?
- Kaj boste naredili, da se incident ne ponovi?
- Kje dobimo uradne informacije?

Spoznano, naučeno

- Nujen (in zagotovljen) je bil „odklop“ – od medijev in dnevnih nalog
- Pravilo 7±2 je držalo
- v času incidenta obstaja visoka stopnja strahu in nejasnosti
  - večja občutljivost ob hkratni večji možnosti nastopa nespoštljivosti itd.
- del javnosti, tudi strokovne, bo vedno nastopal sovražno in agresivno
  - Odziv bi bil brez nadzora občasno neracionalen, temelječ na emocijah
- izjemno smo bili previdni pri obljubah
- komunikacijski načrt za primer varnostnega incidenta bi lahko bil bolje pripravljen
  - vloge, odgovornosti (RACI)
  - kdo, kdaj, komu, kako, kdaj in kako pogosto… bo kaj povedano

Povzetek

- Izjemno veliko naučenega
- Težko je opisati izjemno pomembnost komunikacije
  - še posebej v fazi analize je izredna pomembna hipna medsebojna obveščenost
    - ožja skupina je imela en komunikacijski kanal: vsi vse vemo
  - linija poročanja mora biti jasna
  - jasno mora biti kdo vodi obravnavo incidenta (koordinacija), kdo sprejema odločitve
- Komunikacija je „zimzelena tema“: vedno je lahko boljša!