Osveščanje uporabnikov

V današnjem času, ko do podatkov dostopamo in podatke dajemo preko različnih medijev, moramo uporabniki imeti določeno distanco tako do dajanja podatkov, kot do prevzemanja podatkov v vire ali od virov, ki jih ne poznamo. Varovanje ali nevarovanje osebnih podatkov je povezano z našim znanjem ali neznanjem, previdnostjo ali naivnostjo, ...

Ravnati moramo torej samozaščitno in odgovorno. Kako naj ravnamo in kako naj se obnašamo pa je mogoče najbolje prikazano v virih, ki so navedeni na naslednji strani dokumenta. Za svoje in tuje osebne podatke smo v prvi vrsti odgovorni sami, ne glede na to, ali smo zaposleni pri upravljavcu ali pri obdelovalcu osebnih podatkov, oziroma ko smo upravljavec in obdelovalec lastnih podatkov sami.

Predlagani viri

Linki do glavnih virov, ki so uporabljeni v tem gradivu:

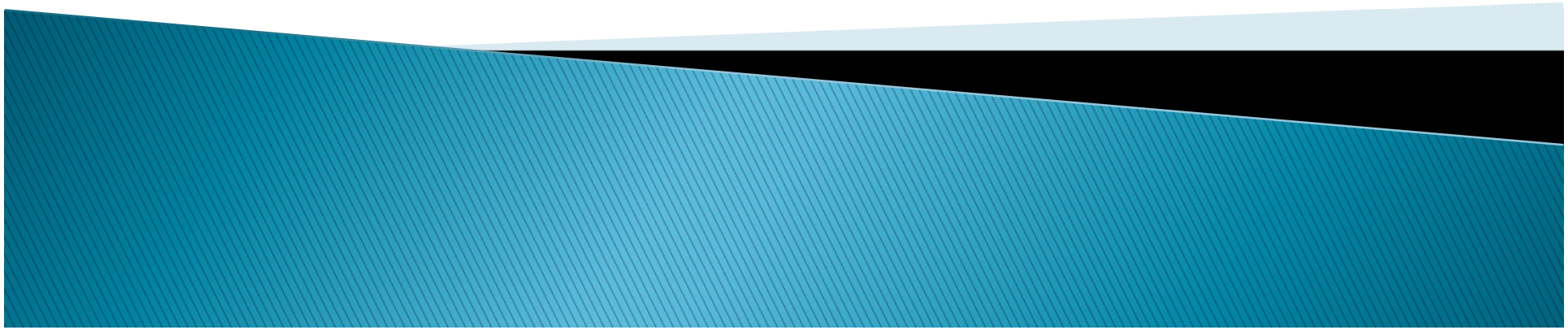
https://www.cert.si/
https://www.varninainternetu.si/
https://blog.radware.com/security/
https://safe.si/
https://www.sisplet.com/
https://www.acronis.com/en-eu/
https://www.istor.net/

Iztok Maver
Zaporedna številka potrdila dodatne kvalifikacije
53/2018-1975/3

Varstvo osebnih podatkov

Varstvo osebnih podatkov je temeljna človekova pravica

<u>Republika Slovenija:</u>
Ustava RS – 38. člen
Zakon o varstvu osebnih podatkov (ZVOP-1)
Področni zakoni, ki ostanejo v veljavi
Uredba 2016/679/EU – GDPR se uporablja neposredno od 25.5.2018



Varstvo osebnih podatkov iz vidika informatike in ravnanja s podatki

Živimo v dobi informatike, kjer smo dosegljivi 24 ur na dan, torej kjerkoli in kadarkoli. Službene podatke prejemamo po e-pošti, ki jo beremo na mobilnih telefonih in odgovarjamo po mobilnih telefonih, ali po tablicah in prenosnikih, ki so priključeni na WiFi omrežja hotela, kjer počitnikujemo.

Naši službeni podatki se nahajajo na spletnih straneh podjetij ali drugih organizacij, katerih profesionalni ali podporni člani smo.

Podatke dajemo na razpolago raznim socialnim omrežjem, ki nas želijo spremljati tako preko navad, preko aplikacij, preko slik, preko všečkov,..

Ne čudite se torej, če boste kdaj tarča. S samozaščitnim ravnanjem poskrbite, da to ne boste ne vi, ne vaši bližnji, ne sodelavci in ne tisti, za katere pri svojem delu skrbite.

Informacijska tehnologija vdira v našo zasebnost.

Švicarski proizvajalec zdravil Novartis želi v letu in pol dobiti odobritev za uporabo tablet z vgrajenimi mikročipi, poroča Reuters.

Skrb za zasebnost

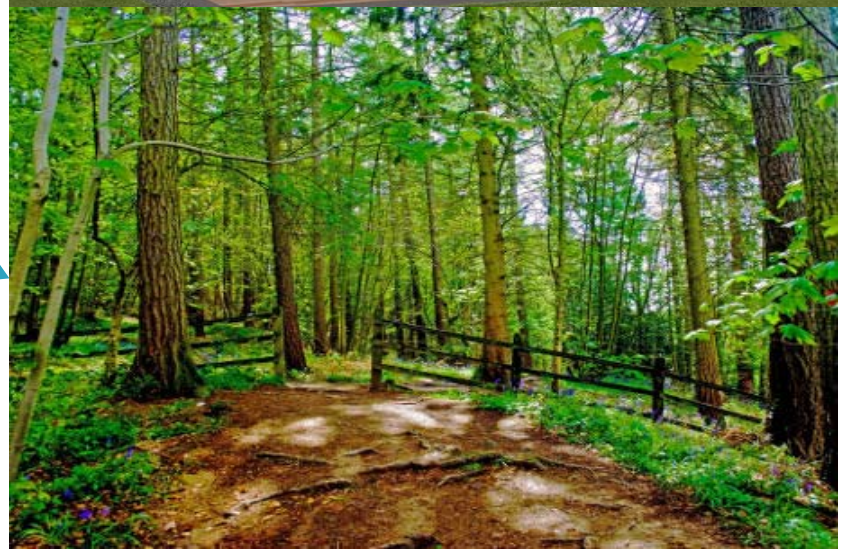
Strah. Tablete s čipi so skeptiki na spletu že označili za korak k popolnemu nadzoru družbe. Skrb za varnost pri prenosu podatkov, ki jih bo zbral čip, pa je tudi ključni pomislek regulatorjev. Čip se bo aktiviral ob stiku z želodčno kislino, za začetek pa bo nadzoroval, kdaj je bolnik zdravilo vzel in ali je količina pravilna.

Vir: https://www.zurnal24.si/svet/iz-zelodca-na-mobilnik-101280 – www.zurnal24.si

Krogi zasebnosti

- Dom,sprehod,..pričakovana zasebnost

1. Krog zasebnosti



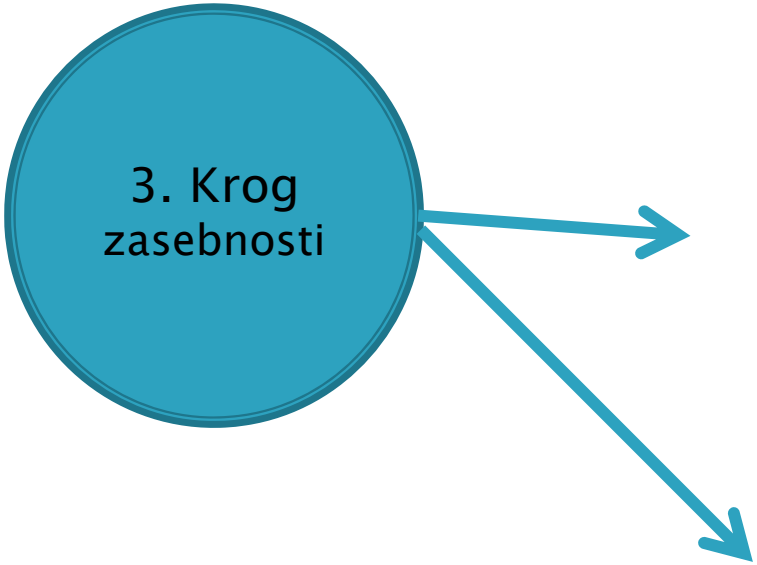
Krogi zasebnosti

- Absolutne in relativne javne osebe (poslanci, manekeni, TV in radijski voditelji, pevci,.., javna mesta, trgovine,..Vdora je več.

2. Krog zasebnosti

Krogi zasebnosti

- Veljajo enaka pravila kot v 2. krogu zasebnosti



Informacijska zasebnost

Komunikacijska zasebnost

Lokacijska zasebnost

Zasebnost: vir https://sl.wikipedia.org/wiki/Zasebnost

- **Teorije o zasebnosti**
- Glede na to, da je zasebnost subjektiven pojem,[3] poznamo tudi več definicij zasebnosti.
- Med prve štejemo Aristotelovo ločevanje javne in zasebne sfere (oikos in polis). Zasebnost je tudi biblična tematika, saj prikaže sramoto ob posegu v zasebnost, npr. ko Adam in Eva spoznata, da sta gola (Milton Konvitz v Wagner DeCew 1997: 11).
- Moderni koncepti opažajo oženje zasebne sfere: »Družina postaja čedalje bolj zasebna, delovno in organizacijsko okolje pa vedno bolj javno«.[4] Hannah Arendt opisuje zasebno sfero kot področje, »kjer je posameznik varen in skrit pred svetom«.[5] Če se zasebna sfera zoži le na intimo, posamezniku ostane zgolj lastna subjektivnost, to pa vodi v razčlovečenje, deindividualizacijo posameznikov in s tem v »usodno, sterilno pasivizacijo«.[6]
- Sykes meni: »Nekateri pravijo, da je zasebnost bistvena za biti človek, vendar je v resnici povsem mogoče biti človek brez zasebnosti. Bolj točno je reči, da je zasebnost nujna za biti svoboden človek«.[7]
- S pravnega vidika zasebnost zaradi svoje subjektivnosti ni nedvoumno ali jasno definirana. Tudi morebitno definiranje bi se lahko v določenem trenutku izkazalo za preozko, zato se v vsakem posameznem primeru sodnega spora tehta pravica do zasebnosti nasproti drugi pravici. Pravica do zasebnosti je sicer definirana kot osebnostna pravica, v kateri se združuje vrsta pravic v zvezi s človekovo osebo in njegovimi osebnimi razmerji. Pravica je, tako kot druge osebnostne pravice, osebna in nepremoženjska. Tudi zanjo je značilno, da pripada posamezniku kot sestavni del njegove osebnosti, ki jo sočasno tudi varuje, pri čemer je varovan tudi njegov odnos do drugih.[8]
- **Področja zasebnosti**
- Zasebnost lahko razdelimo na več področij, na:
- **informacijsko zasebnost**: zajema zbiranje in upravljanje z osebnimi podatki in jo poznamo tudi kot varovanje osebnih podatkov,
- **telesno zasebnost**: pokriva področje, povezano z genetskimi in drugimi preiskavami telesnih tekočin in/ali tkiv ter odprtin,
- **komunikacijsko zasebnost**: zagotavlja zasebnost pošte, telefonskih pogovorov in drugih oblik sporazumevanja in
- **zasebnost v prostoru**: omejuje poseganje v zasebnost na delovnem mestu ali doma.

Osnovna načela obdelave osebnih podatkov

1. Zakonitost
2. Pravičnost
3. Preglednost
4. Omejitev namena
5. Minimizacija – najmanjši potreben obseg podatkov
6. Točnost
7. Omejitev shranjevanja
8. Celovitost
9. Odgovornost upravljavca

Pomen informacijske varnosti

- Informacije predstavljajo vrednost za podjetje, organizacijo, zavod,...in omogočajo delovanje poslovnih procesov.
- Nižja je varnost, večje je tveganje za poslovanje.
- Obstoj tveganja z zlorabo zaradi zunanjih ali notranjih vdorov.
- Informacije predstavljajo vrednost za posameznika: slike, spomini, certifikati, plačila in naročanje preko spletnih aplikacij in banke,...

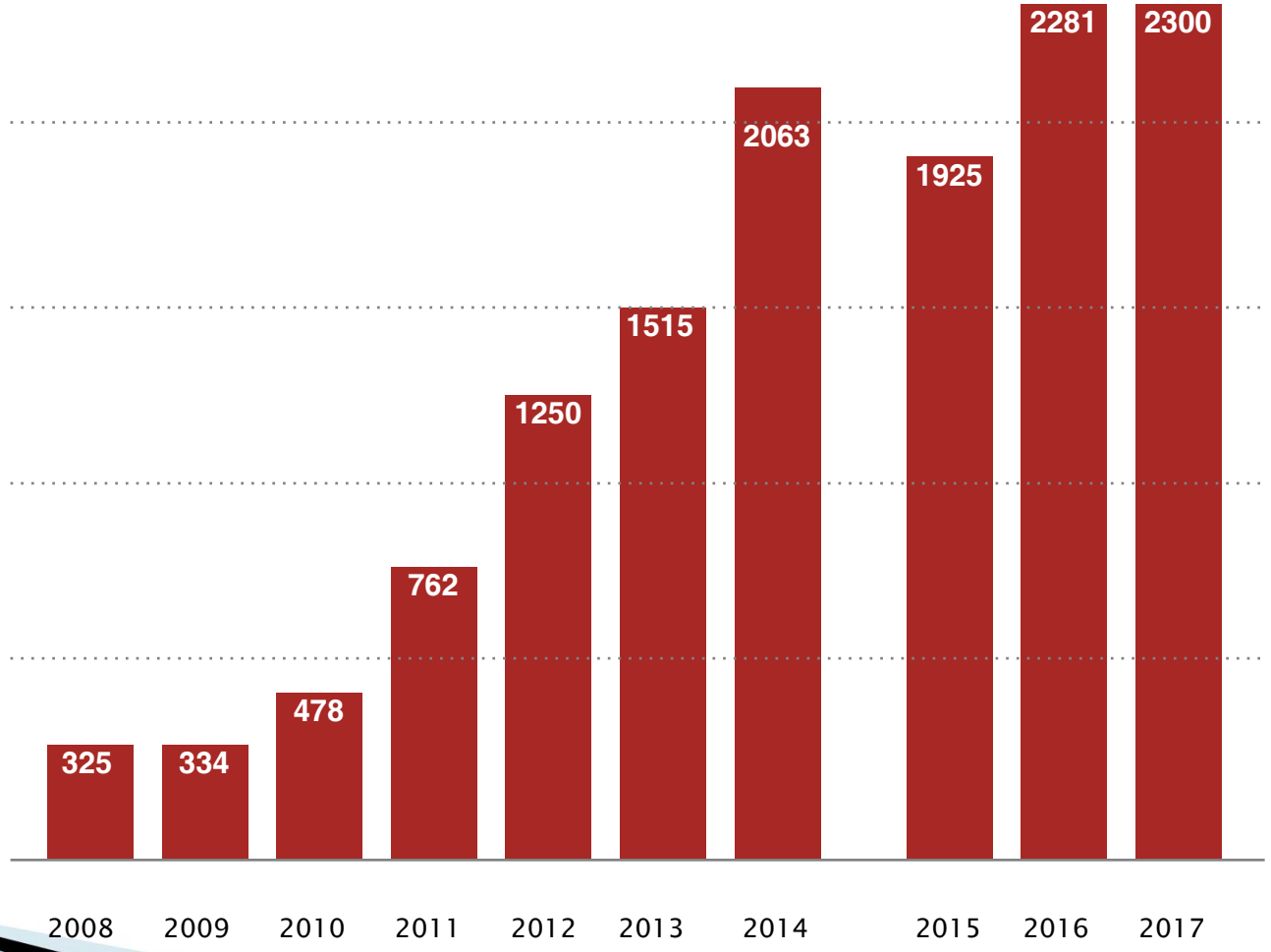
Socialni inženiring

Social Engineering Specialist

Because there is not patch for human stupidity.

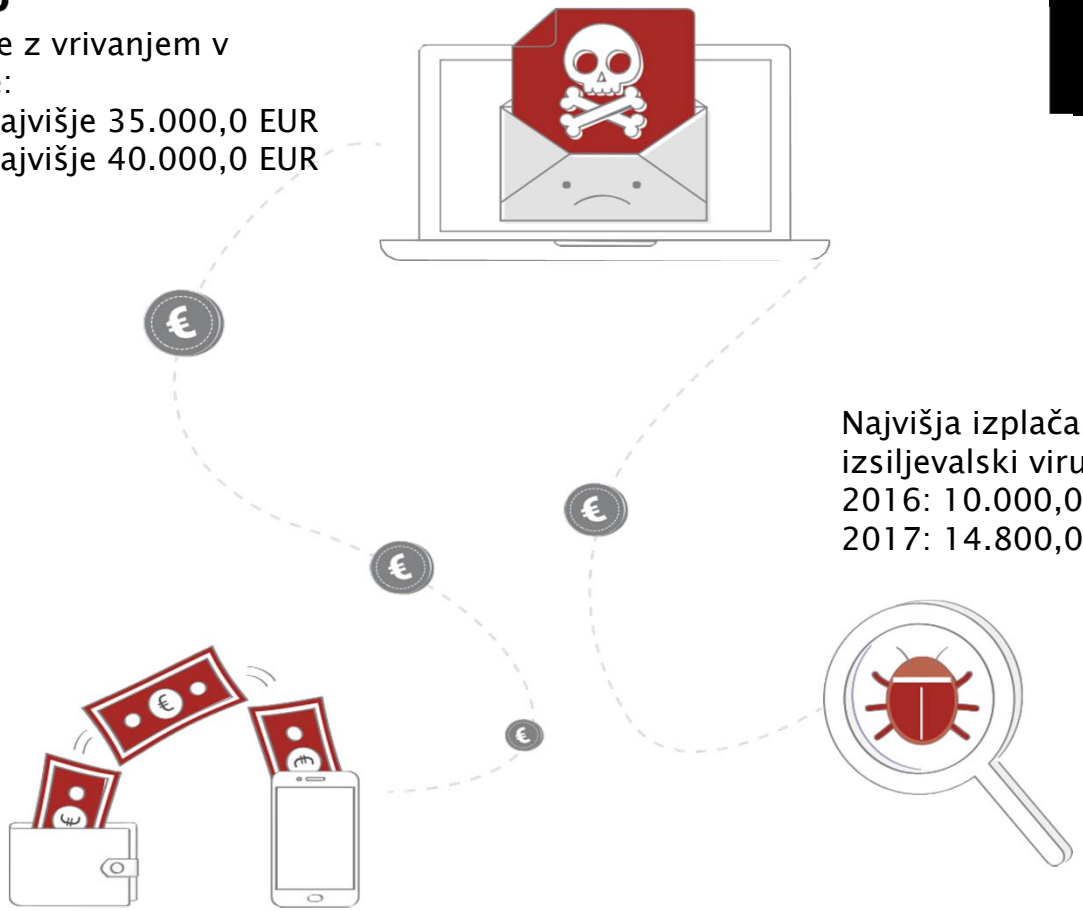
Kako sami pomagamo napadalcem?

Število obravnavanih incidentov si-cert na letni ravni



Oškodovanja

Povprečno oškodovanje z vrivanjem v poslovne komunikacije:
2016: 19.200,0 EUR, najvišje 35.000,0 EUR
2017: 13.640,0 EUR, najvišje 40.000,0 EUR

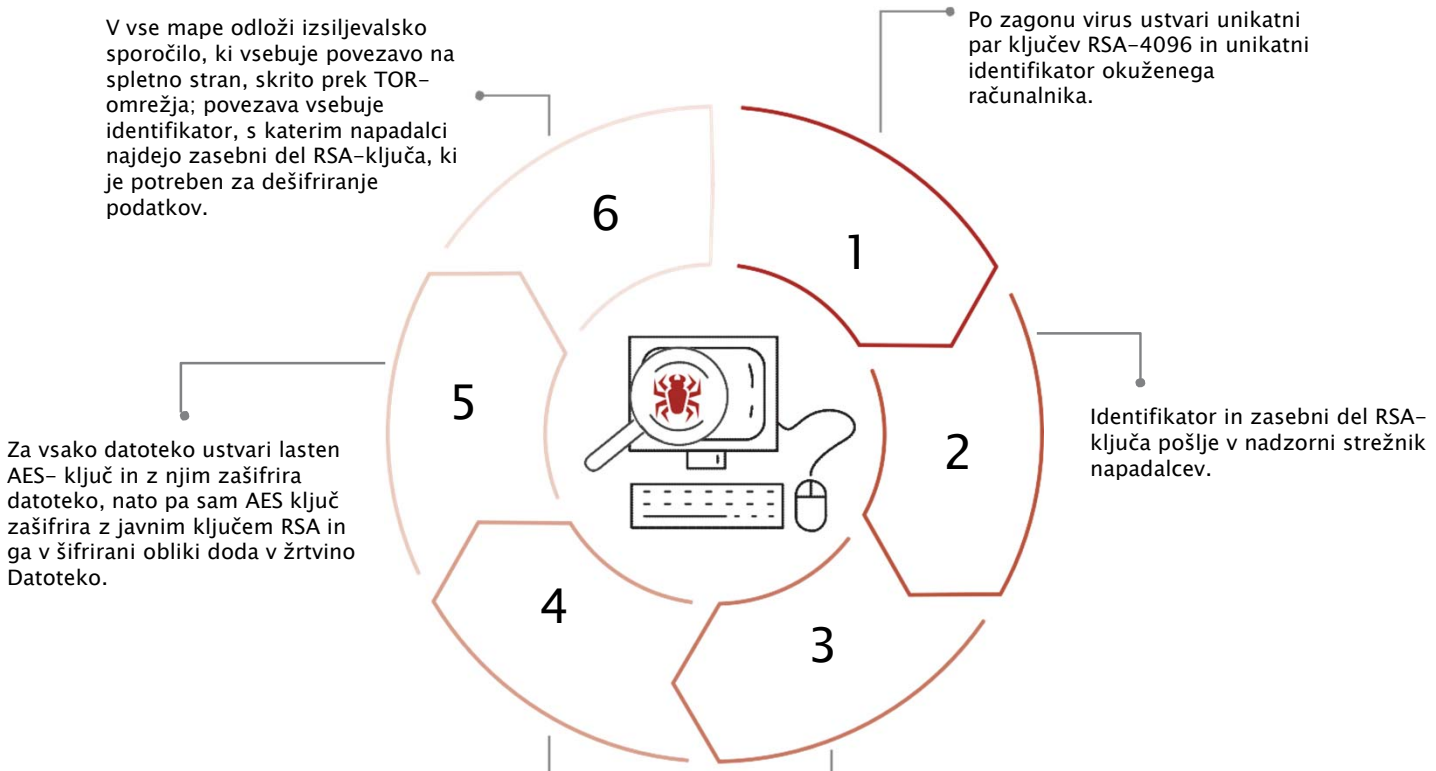


Najvišja izplačana odškodnina za izsiljevalski virus:
2016: 10.000,0 EUR
2017: 14.800,0 EUR

Najvišje oškodovanje pri Nigerijski prevari:
2016: 100.000,0 EUR
2017: 20.000,0 EUR

Kako deluje izsiljevalski virus

Razvoj izsiljevalskih virusov skozi nekaj let je pripeljal do postopka, ki ga uporabljajo skoraj vse sodobne različice:



1. Po zagonu virus ustvari unikatni par ključev RSA-4096 in unikatni identifikator okuženega računalnika.
2. Identifikator in zasebni del RSA-ključa pošlje v nadzorni strežnik napadalcev.
3. Zasebni del RSA- ključa izbriše iz računalnika.
4. Naredi seznam vseh dostopnih datotek na dosegljivih diskovnih pogonih.
5. Za vsako datoteko ustvari lasten AES- ključ in z njim zašifrira datoteko, nato pa sam AES ključ zašifrira z javnim ključem RSA in ga v šifrirani obliki doda v žrtvino Datoteko.
6. V vse mape odloži izsiljevalsko sporočilo, ki vsebuje povezavo na spletno stran, skrito prek TOR-omrežja; povezava vsebuje identifikator, s katerim napadalci najdejo zasebni del RSA-ključa, ki je potreben za dešifriranje podatkov.

Načini širjenja izsiljevalskega virusa

Kampanje izsiljevalskih virusov se ponujajo na črnem trgu kot storitev in okužbe se širijo prvenstveno s priponkami v elektronski pošti. Te so lahko različnih oblik: kot navidezne PDF-datoteke, kot dokumenti programov Microsoft Office z makri ali kot ZIP-arhivi s kodo javascript. Manj pogost način je okužba v mimohodu (angl. drive-by download) s kakšno od vdiralskih orodjarn (angl. exploit toolkit).

Izsiljevalska okužba preko oglasa

V preteklih dveh letih so na si-cert prejeli več prijav uporabnikov, ki so postali žrtev izsiljevalskega virusa ob prebiranju novic. Napadalci so namreč na novičarsko spletno stran z oglasom podtaknili škodljivo kodo. Ta preveri, ali je v sistemu neposodobljena programska oprema, ki omogoča nepooblaščen dostop in namestitev dodatnih zlonamernih komponent. Podtaknjena koda lahko iz sistema pridobi tudi zaupne informaci- je, gesla in certifikate.

Izsiljevalski virus v imenu predsednika

Aprila 2017 je bilo razposlano večje število elektronskih sporočil v imenu predsednika države, ministric in ministrov ter sporočil o nagradnih igrah trgovskih verig, povpraševanju po storitvah odvetniških pisarn in spremembah rezervacij predavalnic na fakultetah.

Sporočilo je vsebovalo ZIP-priponko, v njej pa je bila datoteka javascript, ki je poskusila v računalnik prenesti izsiljevalski virus.

From: Urad RS [mailto:rs@gov.si]
Sent: Monday, April 24, 2017 11:50 AM
To: Protokol
Subject: Obisk predsednika RS

Pozdravljeni,

Napovedujemo protokolarni obisk predsednika RS v naslednjem tednu.
V priponki posiljamo seznam obiskov po obcinah.

Lep pozdrav

Kako se ubraniti pred izsiljevalskim virusom

VARNOSTNE KOPIJE IN POSODOBITVE

Prva in najučinkovitejša zaščita pred izsiljevalskimi virusi je pravilno zastavljen režim izdelave varnostnih kopij ter ustrezno omejevanje pravic dostopa do skupnih datotek za zaposlene, s čimer se ob morebitni okužbi omeji škoda. Omrežja morajo biti razdeljena na različna območja, kar oteži prehajanje okužb ali njenih posledic med njimi. Sledita redno posodabljanje nameščene programske opreme ter izobraževanje zaposlenih glede obravnave elektronske pošte in odpiranja priponk.

Med zgornjimi ukrepi velja posebej omeniti ločitev komercialno-administrativnega okolja podjetja od morebitnih industrijskih in poslovnih procesov. V prvem je komunikacija po elektronski pošti nujna za delovanje podjetja, zato je treba tudi upoštevati možnost okužbe in računati na začasno izgubo podatkov. Okužba v drugem delu pa lahko pomeni neposreden izpad poslovanja. Tak znan primer napada je bil v letu 2017 na Revoz (https://www.dnevnik.si/1042771832).

Obstoja več odličnih sistemov za zaščito podatkov, od katerih navajamo samo dva ponudnika:

Preslikave telefonov, tablic, računalnikov, strežnikov: https://www.acronis.com/en-eu/
iStor: za hranjenje in enkriptiranje podatkov na dveh lokacijah: http://www.istor.net/
iStor uporablja tudi mobilni operater A1:
https://www.a1.si/velika-podjetja/resitve/varnostne-resitve/istor

Ribarjenje – Phishing

Napadi, usmerjeni na posameznika (tako imenovano zvabljanje ali ribarjenje, angl. phishing), so najpogostejša oblika napada s krajo podatkov, ki storilcu omogočajo dostop do različnih storitev v našem imenu. Napadalci si za svoje žrtve izbirajo naključne ali skrbno načrtovane uporabnike, odvisno od namena samega napada.

Preprostost napada
Med zelo pogosto vrsto phising napada sodi sproročilo o preseženem prostoru na uporabniškem računu.
Sporočilo vsebuje povezavo, preko katere naj bi prostor ustrezno povečali, vendar vodi na lažno spletno stran, ki uporabniško ime in geslo sporoči napadalcu.

Primer dejasnkega ribarjenja po e-pošti:

From: 365 Message Centre <kenichi.inoue@jdc.co.jp> / **napadalec**
Sent: Tuesday, July 3, 2018 12:21 PM
To: Ime priimek ime.priimek@podjetje.si / **cilj napadalca**
Subject: Avoid Account Suspension

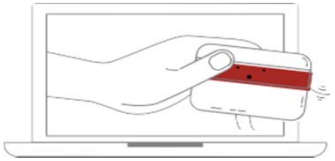
Please confirm your password.
Hi ime.priimek@podjetje.si
Please sign in ime.priimek@podjetje.si from below portal, to retrieve some pending mail(s)
Sign in – **Gumb ali link, kamor se podatke posreduje**
Best Regards,
Note: *We will never ask you for your payment information just account password confirmation.*
2018 © Microsoft Data.

Vdori v poslovno komunikacijo

Postopek prevare

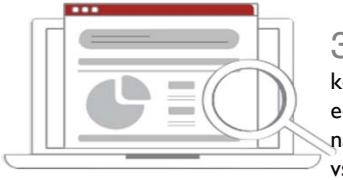
V vseh primerih je zasleden podoben ali identičen vzorec prevare:

2. Prijavijo se v spletni vmesnik za elektronsko pošto in tam nastavijo posredovanje vse pošte na tretji naslov.



4. Elektronsko sporočilo z računom zadržijo, v njem spremenijo podatke o bančnem računu in ga pošljejo žrtvi. Spremenjeno sporočilo pošljejo iz spletnega vmesnika ali pa ustvarijo elektronski naslov, podoben naslovu poslovnega partnerja.

1. Napadalci ukradejo geslo od enega ali več zaposlenih v podjetju.



3. Nekaj časa spremljajo komunikacijo. Ko ugotovijo, da mora eden od partnerjev plačati račun, nastavijo dodatne filtre in preusmerijo vso korespondenco k sebi.

5. Spremenjeni bančni račun pripada denarni muli. Ko je denar nakazan, ga ta po navodilu napadalcev takoj dvigne in po drugem kanalu posreduje naprej. Sled za denarjem se pri tem zelo hitro izgubi.

Izsiljevalski virus NotPetya ali kibernetsko orožje NSA

Kibernetsko orožje ameriške agencije NSA

Eternalblue je koda, ki izkorišča ranljivost Microsoftove implementacije protokola SMB in omogoča oddaljeno nameščanje stranskih vrat z orodjem DoublePulsar. Obe orodji sta del arzenala ameriške agencije NSA, javnosti pa ju je razkrila hekerska skupina Shadow Brokers, ki je ta orodja prodajala po internetu.

Junija 2017 je sledil izbruh izsiljevalskega virusa NotPetya/Petrwrap. Tudi ta se je z uporabo izkoriščevalske kode Eternalblue širil znotraj lokalnih omrežij, vseboval pa je še kodo za zbiranje gesel v okuženih računalnikih (mimikatz), ki je povečala možnost za okužbo drugih računalnikov v lokalnem omrežju. Poznejša analiza je pripeljala do zaključka, da je izsiljeval ska podoba virusa le krinka in da je zelo verjetno namen kode povzročanje zmede in škode. Virus je prepisal master boot record in začetne sektorje vseh diskov v okuženih računalnikih. Začetni vektor okužbe je bila nadgradnja v Ukrajini zelo razširjenega davčnega programa M.E.Doc; tam je bilo zaznanih tudi daleč največ okužb. Na SI-CERT-u so prejeli le dve prijavi uspešnih okužb v Sloveniji in nekaj vprašanj o zaščiti.

NotPetya ni vseboval stikala za izklop, ampak lokalno »cepivo«: datoteko C:\Windows\perfc. Ko ste jo ustvarili v računalniku in jo zaščitili proti pisanju, ste bili imuni proti okužbi.

Oddaljeni dostop

Oddaljeni dostop se uporablja za delo na daljavo, običajno po protokolu Windows Remote Desktop (RDP) za zaposlene ali po Secure Shell (SSH) za skrbnike strežnikov ali vzdrževalce opreme. Kadar ne namestimo dodatne zaščite, sta uporabniško ime in geslo pogosto edini oviri nepooblaščenim očem. V omrežju pa najdete sisteme brez gesel ali takšne, pri katerih se gesla najdejo z iskanjem po prilagojenih slovarjih (angl. dictionary attack).

Potek napada
1. iskanje dostopnih sistemov,
2. dostop brez gesla ali
3. iskanje s prilagojenimi slovarji,
4. zbiranje gesel iz pomnilnika (mimikatz) -> vdor v druge sisteme v omrežju,
5. ustvarjanje novih uporabnikov, kraja podatkov (APT), namestitev bota, bančnega trojanca ali skript za pošiljanje neželene pošte (motiv odvisen od tarče/storilca),
6. šifriranje podatkov z BitLockerjem -> zahtevana odkupnina.

Rešitve:
uporaba VPN ali IPSec za oddaljeni dostop,
zapletena gesla, redno spremljanje dnevnikov in zanesljive varnostne kopije.

IOT – internet of things:
napadi preko pametnih naprav

Največji napadi onemogočanja so bili izvedeni z botnetom Mirai, ki je izrabljal omrežne naprave, predvsem spletne kamere in domače usmerjevalnike na osnovi operacijskega sistema Linux. Proizvajalci teh so uporabljali privzeta gesla in tako omogočili preprost prevzem nadzora nad napravami in njihovo zlorabo za napade onemogočanja. Največji napadi so bili usmerjeni na spletno mesto preiskovalnega novinarja Briana Krebsa, na francoskega internetnega ponudnika OVH in ponudnika DNS-storitev Dyn.

Slovenske naprave v Botnetu MIRAI
Novembra 2017 je enajst internetnih naslovov iz Sovenije pripadalo botnetu Mirai. Si_Cert je obvestil ponudnike, ti pa končne uporabnike.

IOT – internet of things:

Zasebnost, ranljivost in zanesljivost so tri glavna vprašanja, ki se pojavljajo skoraj za vsako pametno napravo, ki je trenutno na trgu, vendar se potrošniki še vedno nepremišljeno in izredno hitro odločajo za avtomatizacijo svojih domov.

IOT – internet of things:

Nikoli ne mislite, da ste varni!

7 najbolj neverjetnih vdorov:
https://blog.radware.com/security/2018/05/7-craziest-iot-device-hacks/

Z zlatimi lasmi do pasu in z glaskom, namenjenim nedolžnim otroškim srčkom, je lutka Cayla navdušila milijone otrok po vsej Nemčiji. V resnici je lutka postala **"nezakonit vohunski aparat",** ki ga je bilo treba nemudoma uničiti, v skladu z navodili nemške zvezne omrežne agencije – Germany's Federal Network Agency.

Ko hekerji nadzorujejo Caylo preko funkcije Wi-Fi, lahko uporabijo njene kamere in mikrofone, da vidijo in slišijo vse, kar počne Cayla, kar hekerjem omogoča, da spremljajo lokacijo in otroke ter odrasle ljudi na tej lokaciji. Vsak zase si lahko predstavlja, kaj to pomeni in kašen vdor v zasebno življene je to.

Zaskrbljujoče je, da se varnost pri teh napravah zanemarja. Te naprave namreč hekerji **„ povlečejo v svojo vojsko "** kontroliranih naprav, znanih kot botnet. Iz teh naprav se namreč izvajajo napadi naprej.

https://sl.wikipedia.org/wiki/Mariposa_botnet
https://www.racunalniske-novice.com/novice/sporocila-za-javnost/eset-odkril-in-unicil-botnet.html
https://www.monitor.si/novica/botnet-pocetveril-rabo-tora/148077/

IOT – internet of things:

Nikoli ne mislite, da ste varni!

7 najbolj neverjetnih vdorov:
https://blog.radware.com/security/2018/05/7-craziest-iot-device-hacks/

Ocean's 14?

Ko gre za krajo podatkov, bodo hekerji uporabili vsa sredstva, ki so jim na voljo. Igralnice so med najbolj varnimi organizacijami in objekti na tem planetu, zato se je skupina hekerjev odločila, da bo s pomočjo termometra v akvariju, v preddverju igralnice, vdrla v IT sistem igralnice.

Po dostopu do omrežja igralnice so hekerji postavili bazo in jo prenesli preko termostata. Ta vdor morda ni bil tako drzen kot v filmu Ocean's Eleven (https://en.wikipedia.org/wiki/Ocean%27s_Eleven), toda za igralnico, ki je imela svoje osebne podatke kompromitirane, je bil ta vdor podoben izgubi desne roke.

Akvarij morskih psov v zalivu Mandalay, ki nima zveze z zgoraj opisano igralnico.
Izvor: MGM Resorts
https://www.mgmresorts.com/en/things-to- do/mandalay-bay/shark-reef-aquarium.html

IOT – internet of things:

Nikoli ne mislite, da ste varni!

7 najbolj neverjetnih vdorov:
https://blog.radware.com/security/2018/05/7-craziest-iot-device-hacks/

Tiskanje v pisarni je lahko tvegano početje. Izpostavljamo tveganje, da lahko vaš sodelavec pregleda ali vpogleda v dokument, ki je oseben, zaupen ali strogo zaupen. Najhuje je, če v mrežno povezani tiskalnik v vaši organizaciji vdre digitalni napadalec.

Uspešni vdori v tiskalnike omogočajo hekerjem, da preko pomnilnika tiskalnika dostopajo do tiskalniških opravil, ki vsebujejo občutljive datoteke kot so pogodbe, podatki podjetja ali podatki o bolniku. Poleg tega so lahko ogrožena tudi gesla podjetja.

Vir: PC Mag
https://www.pcmag.com/article2/0,2817,2411967,00.asp

IOT – internet of things:

Nikoli ne mislite, da ste varni!

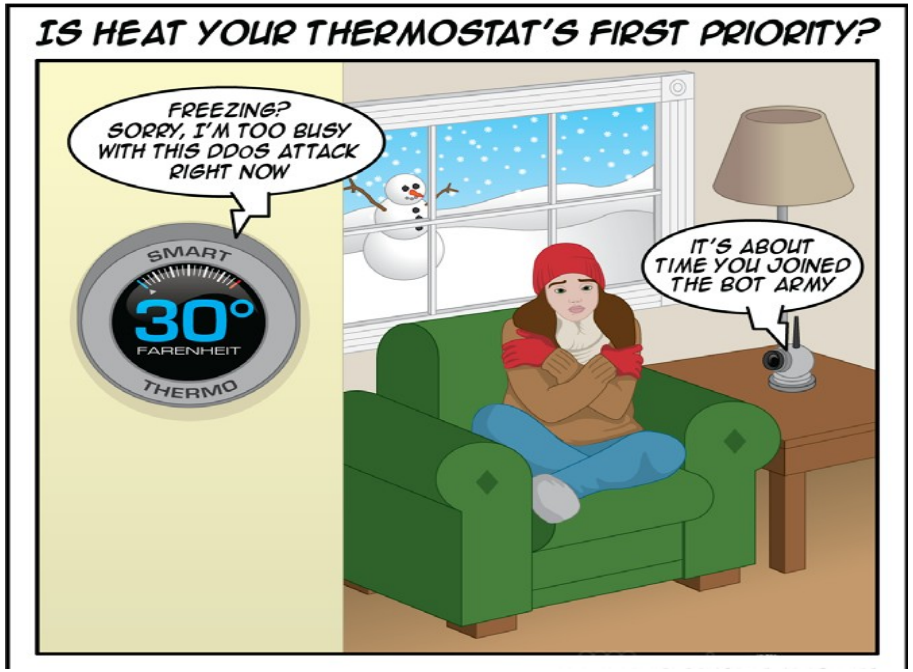
7 najbolj neverjetnih vdorov:
https://blog.radware.com/security/2018/05/7-craziest-iot-device-hacks/

Nedelovanje ogrevanja.

Nova generacija na internet priključenih termostatov je postala trajni in najljubši cilj hekerjev, kot je razvidno iz prej omenjenega primera igralnice. Leta 2016 so hekerji „zamrznili“ prebivalce Lappeenranta na Finskem, ko so preko termostatov uspeli prevzeti nadzor nad ogrevalnimi sistemi v dveh stanovanjskih zgradbah.

V poskusu boja proti napadu so se okoljski sistemi ponovno zagnali in nato zataknili v neskončno zanko, ki je pustila prebivalce na hladnem skoraj cel teden.

https://thehackernews.com/2016/11/heating-system-hacked.html



IOT – internet of things:

Nikoli ne mislite, da ste varni!

7 najbolj neverjetnih vdorov:
https://blog.radware.com/security/2018/05/7-craziest-iot-device-hacks/

Resnična nočna mora – Prevzem nadzora nad otroškimi opazovalnimi napravami

Nadzorni monitorji za otroke so že precej stara in znana tehnologija. Začeli so se s preprostimi enosmernimi radijskimi oddajniki, ki so se razvili v prefinjene WiFi-omogočene pametne naprave, ki imajo sprejemnik, video kamero, infrardeči vid in številne druge zmogljivosti.

Te iste visokotehnološke zmogljivosti so te točke varnosti za malčke spremenile v pravo nočno moro. Hekerji iščejo priložnosti in v te komajda zavarovane naprave lahko vdrejo praktično kjerkoli na svetu preko Wi-Fi povezav teh naprav. Baby monitorji so odličen primer, kako lahko na videz brezhibne in nedolžne naprave povezane z internetom združijo hekerji, da začnejo množične napade z zavrnitvijo storitve – DDoS napadi.

https://www.lifewire.com/is-your-baby-monitor-being-hacked-2487802

https://en.wikipedia.org/wiki/Denial-of-service_attack

https://servicemasteranchorage.com/2016/02/29/128/oh-my-gosh-face/

IOT – internet of things:

Nikoli ne mislite, da ste varni!

7 najbolj neverjetnih vdorov:
https://blog.radware.com/security/2018/05/7-craziest-iot-device-hacks/

Oddaljen prevzem nadzora nad avtomobilom

Strokovnjaka za avtomobilsko kibernetsko varnost Charlie Miller in Chris Valasek sta v zadnjih letih naredila valove , s katerimi sta vdrla v Chrysler Jeep Cherokee. Začela sta pošiljati oddaljene ukaze prek sistema GPS. Dokazano je, da heker lahko oddaljeno obrne volan ali aktivira parkirno zavoro in to vse pri hitrostih, kot so recimo na avtocesti. Dokazan koncept, ki so se ga bali je, da bi vas lahko kdo z vašim avtomobilom spremenil v lutko za testiranje trka.

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

https://www.youtube.com/watch?v=MK0SrxBC1xs

IOT – internet of things:

Nikoli ne mislite, da ste varni!

7 najbolj neverjetnih vdorov:
https://blog.radware.com/security/2018/05/7-craziest-iot-device-hacks/

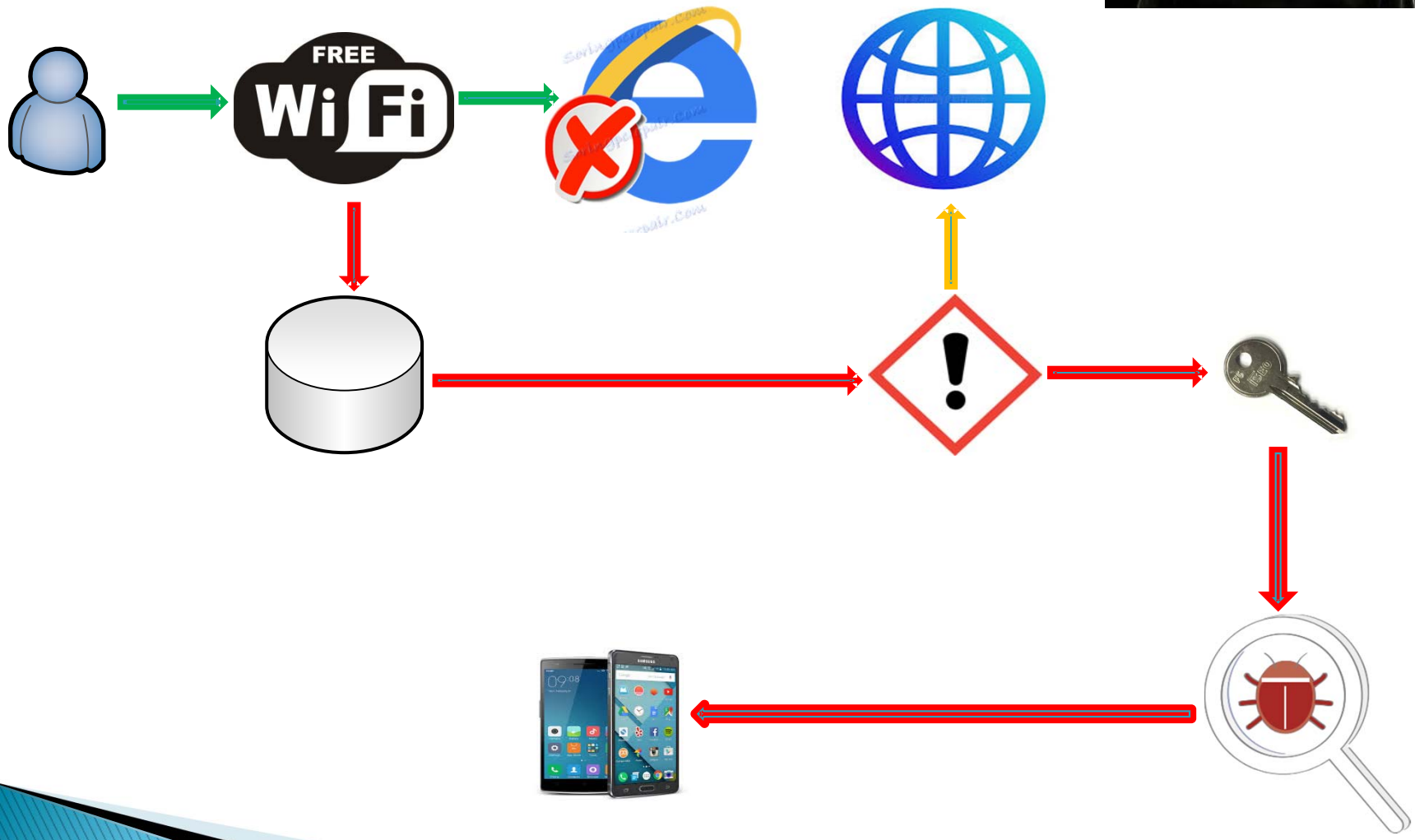
Ne tako pametne, pametne televizije. Ali vi gledate televizijo, ali televizija gleda vas?

Pametne televizije predstavljajo večino prodaje novih televizij. Po podatkih tržnega raziskovalnega podjetja IHS Markit je 69% vseh novih televizij, dobavljenih v Severni Ameriki leta 2017, možno priključiti na internet. Ta odstotek se bo še povečal v letu 2018. Internetna povezava prinaša veliko privlačnih funkcij, kot so zmožnost pretakanja vsebin prek priljubljenih aplikacij, kot so Hulu in Netflix, ter možnosti hitrega iskanja vsebine z glasovnimi ukazi.

Te televizije pa prinašajo varnostne nočne more, kot jih imajo podatkovni centri in podjetja, direktno v vašo dnevno sobo. Ti televizorji imajo precej zbranih podatkov . Ker omogočajo dostop do interneta to pomeni, da je mogoče vanje vdreti in ogroziti te podatke. Hekerji lahko spremenijo kanale, sprožijo pornografsko ali žaljivo vsebino na TV, ali pa zbirajo podrobne podatke o uporabnikih televizorja. Ker je s TV –jem večji del potrošnikov vse bolj povezanih doma, ne bo dolgo trajalo, da heker vzpostavi nadzor tudi nad drugimi pametnimi napravami, od prej omenjenih termostatov , fotoaparatov , pralnih strojev , zvočnikov itd..

Predstavljajte si sproščujoči večer gledanja televizije v soboto zvečer, ko se bo vaš Voyo program spremenil v domači pekel, ko bo televizor spreminjal kanale, ko bo pralni stroj preobremenjen s pranjem perila, ko bo štedilnik pričel sam kuhati vodo, ko bo hladilnik zamrznil ali odtajal hrano in ko bo sredi zime vaše gretje prenehalo delati,..

Preusmeritev na lažno spletno stran, ali dostop do interneta



Učinkovito ravnanje z gesli

Učinkovito ravnanje z gesli

Primeri, kako se z gesli ne ravna!

https://youtu.be/opRMrEfAIiI?t=41

https://www.varninainternetu.si/mocno-geslo/

Na spletni strani https://haveibeenpwned.com/ lahko za vaš elektronski naslov preverite, ali se morda nahaja v kakšnih zlorabljenih bazah podatkov. Če se, potem povsod zamenjajte geslo, ki ste ga uporabljali za to storitev.

Vir: https://www.varninainternetu.si/mocno-geslo/

Učinkovito ravnanje z gesli

1.) Vsa privzeta gesla spremenite ob prvi prijavi v sistem.

2.) Vsak uporabnik mora imeti unikatno geslo za dostop.

3.) Dobrodošlo je, če je geslo iz velikih in malih črk, številk in nealfanumeričnih znakov.

4.) V geslih ne uporabljajte svojih osebnih podatkov, podatkov partnerjev, otrok sorodnikov.

5.) Ne uporabljajte istih gesel za različne račune.

6.) Gesel ne shranjujte nezaščitenih, ne zapisujte jih na listke in ne delite jih z drugimi.

V zadnjem času so popularna takoimenovana pojoča gesla. Gesla so kompleksna, vendar se jih lažje zapomnimo in natipkamo hitreje, kot težka kompleksna gesla:

Primer težkega kompleksnega gesla. Tc.M3.xZv47.
Primer pojočega gesla: Trzinka.Trzinka.NaRaufnkSeJeUsedla.
Primer pojočega gesla: ImamKraveInOvceNaPlanini.
Primer pojočega gesla: SprehodilSemSeMimoVrtaInNazaj.

Uporaba službene elektronske pošte

Za poslovno komunikacijo

Dovoljena je osebna raba (vendar omejeno)

Pošiljanje dokumentov na zunanje osebne ali druge e-naslove?
Možnost izgube zaupnosti informacij!

Delodajalec je lastnik službenega elektronskega naslova

Zaposleni ima svoje pravice, vendar mora delovati po veljavnem pravilniku delodajalca

Problematika lažne elektronske pošte

Obnašanje in komuniciranje na spletu

Pri komuniciranju prek mobilnega telefona in spleta **upoštevaj bonton, bodi strpen in prijazen. Obnašaj se tako, kot želiš, da se drugi do tebe.**

Česar ne bi rekel v živo, ne natipkaj online! Ne skrivaj se za anonimnostjo, za zaslonom. Na spletu smo pogosto lažje nesramni do drugih, saj svoji žrtvi ne gledamo v obraz, to pa ne pomeni, da je tako kaj lažje žrtvi! Poleg tega pa na anonimnost pri takih stvareh ne gre računati, saj puščamo elektronske sledi.

Tudi če kdo pusti svoj telefon dostopen in nezaklenjen, to ne pomeni, da lahko po njem brskaš in ga uporabljaš. V telefonu imamo tudi zasebne fotografije, sporočila in podatke, vsak pa ima pravico do zasebnosti!

Osebo, ki jo želiš fotografirati , s svojim mobilnim telefonom, prej **vprašaj za dovoljenje.** Mogoče ji ni do tega oziroma se počuti neprijetno.

Ne razpošiljaj sporočil, slik, video posnetkov, ki nekomu škodijo. Razpošiljanje posnetkov pretepov, trpinčenja, ki jih sami prejmemo, naprej svojim prijateljem ni sprejeemljivo. S tem se aktivno vključimo v trpinčenje, saj je vsakič, ko si nekdo pogleda ta posnetek, žrtev ponovno žrtev. Taka sporočila brišemo!

Ne peri umazanega perila na spletu. Prepiranje, razčiščevanje sporov, konfliktov, družinskih nesoglasij, nesporazumov s prijatelji znanci in neznanci ne sodi na splet. O teh stvareh se raje pogovorimo v živo, kjer ni tako številčnega občinstva kot na spletu.

Tudi s fantom/punco se ne konča s spremembo statusa na FB. **Za resne stvari**, prekinitev zveze, izražanje sožalja ipd. **je še vedno najprimernejši način iz oči v oči** (pa to ne pomeni prek spletne kamere).

Ko si z nekom v družbi, se posvečaj tej osebi in **ne preverjaj neprestano, kaj se dogaja na tvojem mobilnem telefonu,** Facebooku … Pogovarjanje po telefonu, čekiranje telefona, ko si z nekom v družbi, je nevljudno in gre tudi večini ljudi zelo na živce.

Obnašanje in komuniciranje na spletu

Zvonjenje telefona in/ali pogovarjanje v kinu, gledališču, med poukom, v bolnišnici, na busu … je **nedopustno.**

Ne širi nestrpnosti in sovražnega govora **na spletu!** Širjenje sovražnosti na spletu je kaznivo dejanje.
Ne počni tega, če pa naletiš nanj, prijavi na Spletno oko.

Bonton: https://safe.si/nasveti/obnasanje-na-spletu/spletni-in-mobilni-bonton

Spletno oko: https://www.spletno-oko.si/

Viri: https://safe.si/

Nigerijska prevara

https://www.varninainternetu.si/article/nigerijska-in-loterijska-prevara/

Tako ali podobno e-pošto samo izbrišite!

Primer Nigerijske prevare:

Od: kiyoshi_ogawa196_3@yahoo.co.jp [kiyoshi_ogawa196_3@yahoo.co.jp] v imenu Aloisia Viktoria Eberhartinger [aloisiaa1960@gmail.com]
Poslano: 6. avgust 2018 15:51
Za: aloisiaa1960@gmail.com
Zadeva: Dobro jutro,
Dobro jutro,

Prosimo, ne jezite se, da bi prebrali to sporočilo, ker ste nameravani prejemnik. Videl sem vaš e-poštni naslov prek imenika in sem se obrnil na vas, ker sem vam nujno potreboval pomoč. Moje ime je gospa Aloisia Viktoria Eberhartinger. Sem 57 letna ženska in pravno sem poročena s pokojnim gospodom Petrom Eberhartingerjem. Jaz in moj pokojni mož, kjer so bili državljani Nemčije, vendar smo živeli tukaj v Slonokoščeni obali Zahodne Afrike v zadnjih 28 letih.

Moj pokojni mož je delal z družbo za vrtanje nafte kot izseljenec tukaj na Slonokoščeni obali že več let, preden je umrl zaradi usodne prometne nesreče, ki je ubil njega in njegovega voznika tukaj v Slonokoščeni obali. Jaz in moj pokojni mož sta bila poročena brez enega samega biološkega otroka. Trenutno imam resno bolezen raka dojke in pišem to sporočilo s pomočjo zdravnika tukaj v bolnišnici v Slonokoščeni obali.

Nadaljevanje na naslednji strani:

Nigerijska prevara

https://www.varninainternetu.si/article/nigerijska-in-loterijska-prevara/

Tako ali podobno e-pošto samo izbrišite!

Primer Nigerijske prevare nadaljevanje:

Ko je bil moj pokojni mož živ, je na Švedskem deponiral znesek v višini enega milijona petsto tisoč evrov (1.500.000,00 evrov), ki je podpisal sporazum z banko, da bodo sredstva porabljena za dobrodelne namene, kot so; pomoč materinim dojenčkom, podpiranje cerkvenih dejavnosti in pomoč otrokom, ki nimajo privilegija, da nadaljujejo svoje izobraževanje. Moj mož je sprejel to odločitev za to dobrodelno delo, ker nimamo otroka, ki bo podedoval sredstva v švedski banki in ga vzgojil center za sirotišče v Berlinu - Nemčija, ker v Nemčiji nima družine.

Danes sem stopila v stik z vami, ker me je moj zdravnik obvestil, da se je bolezen raka na dojki najhujša in do naslednjega tedna bodo izvedli resno / smrtonosno operacijo raka, ki ga morda ne bom preživel, ker je bolezen pogoltnila globoko v sistem mojega telesa. Bojim se, da če bom umrl med operacijo naslednji teden, bodo sredstva v švedski banki pozabljena, ker nimam nobenega drugega sorodnika, da bi to zahteval in ne morem najti nobene družine mojega pokojnega moža v Nemčiji.

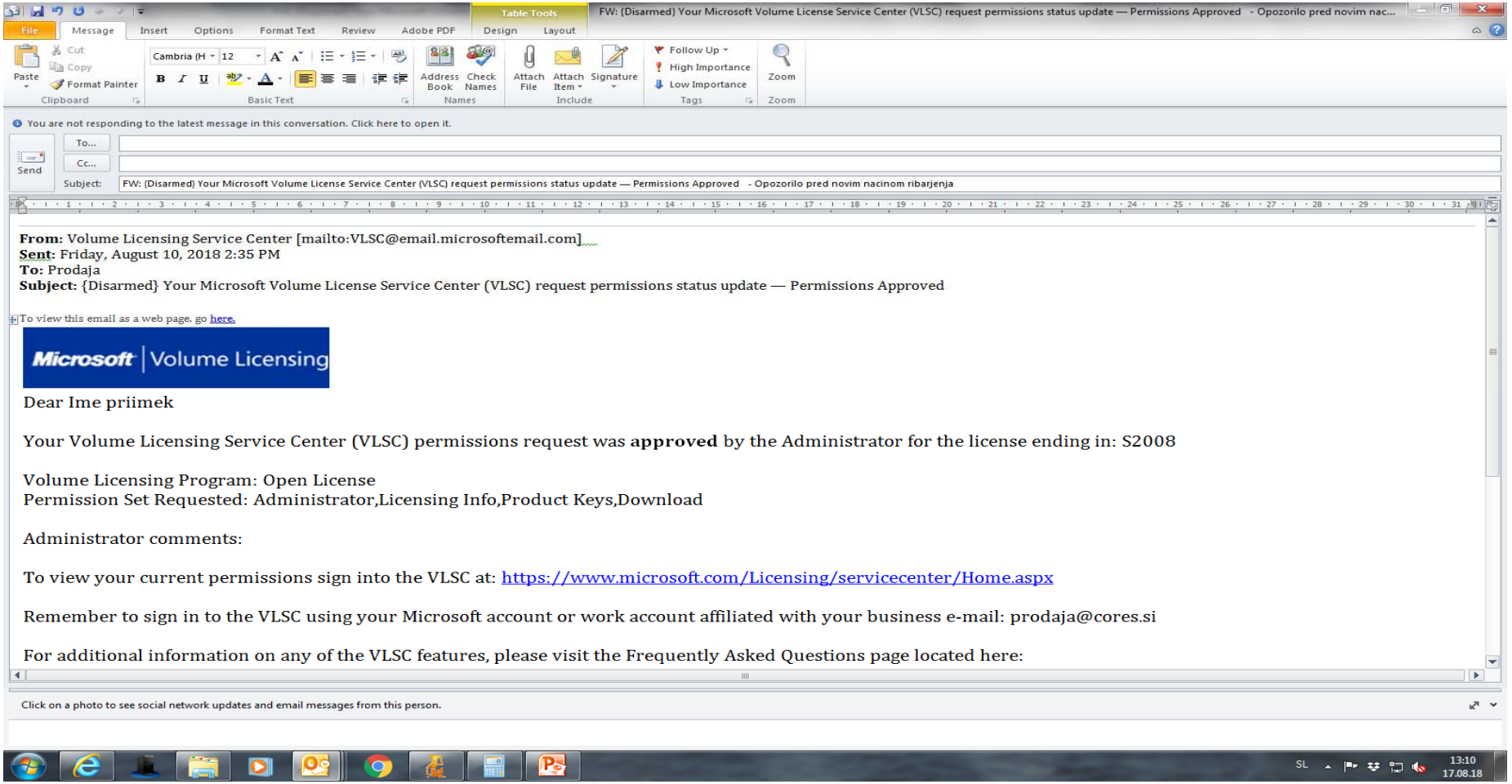
Opomba: Želim, da mi pomagate prenesti sredstva na vaš osebni bančni račun in po nakazilu na vaš bančni račun; zbrali boste 30% (450,000.00 EUR) celotnih sredstev za vašo lastno nadomestilo in uporabite preostalih 70% (1,50, 000,00 EUR), da opravite dobrodelno delo v vaši državi. Prosim, odgovorite mi nujno, če ste zainteresirani, da mi pomagate pri tej transakciji, tako da vam bom poslal več podrobnosti, ker želim, da se sredstva prenesejo pred prihodnjim operacijam naslednji teden, in zelo mi je žal za moj slab Slovenski prevod.

S spoštovanjem,

Ga. Aloisia Viktoria Eberhartinger

Ribarjenje / phishing

https://www.varninainternetu.si/article/phishing-kraja-podatkov/
https://www.cert.si/si/varnostne-groznje/phishing/
Tako ali podobno e-pošto samo izbrišite ali prijavite na si - cert, e-naslov info@cert.si



From: Volume Licensing Service Center [mailto:VLSC@email.microsoftemail.com]
Sent: Friday, August 10, 2018 2:35 PM
To: Prodaja
Subject: {Disarmed} Your Microsoft Volume License Service Center (VLSC) request permissions status update — Permissions Approved

To view this email as a web page, go here.

Microsoft | Volume Licensing

Dear Ime priimek

Your Volume Licensing Service Center (VLSC) permissions request was **approved** by the Administrator for the license ending in: S2008

Volume Licensing Program: Open License
Permission Set Requested: Administrator,Licensing Info,Product Keys,Download

Administrator comments:

To view your current permissions sign into the VLSC at: https://www.microsoft.com/Licensing/servicecenter/Home.aspx

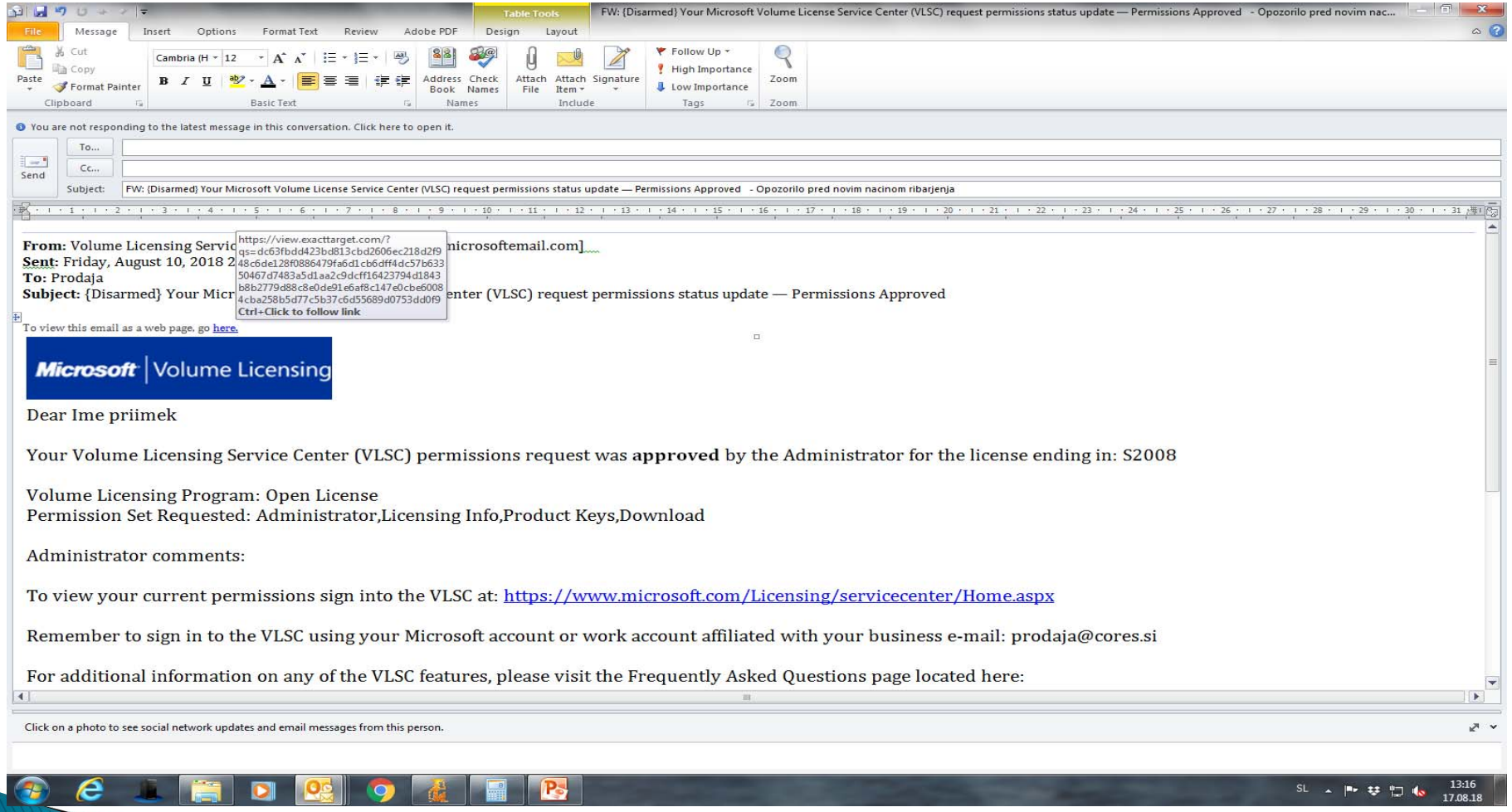
Remember to sign in to the VLSC using your Microsoft account or work account affiliated with your business e-mail: prodaja@cores.si

For additional information on any of the VLSC features, please visit the Frequently Asked Questions page located here:

Zavedajte se, da so hekerji večkrt izredno sofisticirani in vas skušajo zavesti na način, da gre za uradno stran proizvajalca ali ponudnika storitve.

Ribarjenje / phishing

https://www.varninainternetu.si/article/phishing-kraja-podatkov/
https://www.cert.si/si/varnostne-groznje/phishing/
Tako ali podobno e-pošto samo izbrišite ali prijavite na si - cert, e-naslov info@cert.si



Včasih je dovolj, da se z miško približamo linkom v e-pošti in s tem ugotovimo napadalčev izvor. V našem primeru je to https://view.exacttarget.com/? Če niste prepričani v varnost e-pošte, pošljite le to v analizo vašemu sistemskemu skrbniku ali na info@cert.si.

Ali lahko danes plačamo?

https://www.varninainternetu.si/ali-lahko-danes-placamo/

Tako ali podobno e-pošto samo izbrišite ali prijavite na si - cert, e-naslov info@cert.si

From: Stojanka
Sent: Tuesday, July 31, 2018 7:46 AM
To: Marko Toporis <ericbrendon4@gmail.com>
Subject: Re: Nujno!

Dober dan, ne razumem , kaj zelite?
Poklicite me ko boste utegnil.
Lp

Dobite Outlook za Android

On Mon, Jul 30, 2018 at 3:27 PM +0200, „Marko Toporis" <marko.toporis@podjetje.si> wrote:
Ga. Jožica,

Želim poslati mednarodni prenos v višini 12,855.00 EUR
Ali lahko zdaj? Hočem vedeti,
zato bom takoj poslal podatke.

S prijaznimi pozdravi,

Marko Toporis

Poslano iz naprave Samsung

Včasih je dovolj, da se z miško približamo linkom v e-pošti in s tem ugotovimo napadalčev izvor. V tem primeru je to ericbrendon4@gmail.com . Če niste prepričani v varnost e-pošte, pošljite le to v analizo vašemu sistemskemu skrbniku ali na si-cert na info@cert.si.

Gospa je spregledala, že ko je odgovarjala na e-pošto, da je razkrila napadalca, oziroma je odgovarjala napadalcu in ne svojemu direktorju.

Tako e-pošto seveda samo izbrišite.

Pridobitev zaupne dokumentacije preko e-pošte

Običajno se napad izvede tako, da se kreira lažna domena, tarčo posameznika pa se preslepi

Domena podjetja	Lažna domena
www.print.com	www.prlnt.com
E-pošta:	E-pošta
andrej@print.com	andrej@PRINT.com

V tem primeru je torej črka i zamenjana s čkrko l (mali L).

V takih primerih preverite pri gospodu Andreju, ali vam je dejansko poslal elektronsko sporočilo, oziroma zakaj ima domeno napisano z velikimi črkami.

Goljufive spletne strani – primer:

Viagogo ali ViaNOgo – zavajanje in goljufanje potrošnikov na spletu:

http://www.rtvslo.si/zabava/glasba/viagogo-ali-vianogo-zavajanje-in-goljufanje-potrosnikov-na-spletu/444234?fbclid=IwAR3c7p_h-bLNf_N-augPUJRtyWREmAWm-M3iFOZXgjCBu0gg3S3dbTQx6mg

https://www.viagogo.com/si

Raziskava USB ključek

Recimo, da je bil USB ključek dan varnostniku z dopisom: „ Priložen USB ključ sem našel pred vhodom vaše organizacije. Po vsebini sodeč pripada enemu od vaših sodelavcev. Prosim, da mu ga vrnete, saj menim, da se na njem nahajajo pomembni dokumenti.
In podpis.

Na ključku je bila aplikacija, ki je javila sprejemniku, da je bil ključek vtaknjen v računalnik, uporabnik pa je bil istočasno obveščen, da je postal „žrtev“ raziskave.

90% organizacij je ključek uporabilo
10% organizacij je imelo vpeljane varnostne politike ali so podvržene določenem standardu – recimo informatik je preskusil ključek na za to namenjenem računalniku, ki je bil ločen od omrežja, oziroma so ključek enostavno uničili brez preskusa.

Na podlagi raziskave se lahko naredi:

a.) Preverjanje, kaj se v organizaciji dogaja s ključkom
b.) Preverjanje varnostne politike v podjetju
c.) izobraževanje zaposlenih in preverjanje učinkovitosti izobraževanja

Mnenje etičnega hekerja: **„Največji problem so ljudje sami, ker brez razmisleka klikajo da, da, da, naprej ...“**

https://www.rtvslo.si/slovenija/eticni-heker-najvecji-problem-so-ljudje-sami-ker-brez-razmisleka-klikajo-da-da-da-naprej/415999

Kaj tehnološki giganti resnično počnejo z vašimi podatki? Vir: https://www.dataprotection-officer.com

Sledenje žiroskopu vašega telefona, optično prebiranje vaših sporočil in razkrivanje vaših osebnih podatkov tretjim osebam. To so samo tri stvari, s katerimi ste se strinjali, ko ste se prijavili na nekatere aplikacije in spletne strani določenih tehnoloških podjetij.

BBC je v svojih raziskavah ugotovil, da nekateri izmed jezikov, ki se uporabljajo v politikah in pravilnikih o zasebnosti, zahtevajo univerzitetno izobrazbo, da jih lahko razumeš. Ampak, če bi pogledali bolj podrobno, bi bili presenečeni, kako se v resnici uporabljajo vaši podatki.

Vaši lokaciji se sledi – tudi če tega ne dovolite
Mnogi programi zahtevajo dovoljenje, da sledijo vaši lokaciji preko GPS, ampak kot uporabnik lahko to zavrnete. Toda tudi če zavrnete dovoljenje za aplikacijo, lahko še vedno vidijo kje ste. Na primer, Facebook zbira informacije o lokaciji preko GPS, vgrajenega v telefon. Še vedno sledi, kje se gibljete tudi preko IP naslovov, preko prijave ali dogodkov, ki jih obiskujete. Twitter prav tako "zahteva" informacije o vaši trenutni lokaciji: *"Dobimo jih iz signalov, kot so vaš IP naslov ali nastavitev naprave"*. Tako lahko *»varno in zanesljivo nastavite in vzdržujete račun«*.

Podjetja prenesejo svoje podatke na podružnice ...
Ko se strinjate s pogoji in določili, pogosto ne posredujete vaših podatkov tej posebni aplikaciji – obstaja veliko izmenjave podatkov znotraj skupine. Na primer podatki, ki prihajajo iz aplikacije Tinder, se zbirajo v skupni rabi z drugimi člani skupine za ujemanje, ki vključuje druge spletne strani za zmenke OkCupid, Plenty of Fish in Match.com. Tinder pravi, da to počne za *"vzdrževanje, skrb za stranke, trženje in ciljno oglaševanje"* ter za odstranitev uporabnikov, ki kršijo pogoje uporabe. Microsoft je kupil LinkedIn leta 2016 in v skladu s svojo politiko zasebnosti prejme podatke o posamezniku, ko uporablja nekatere druge storitve, ki jih zagotavlja Facebook ali njihova podružnica, vključno z Microsoftom.

Kaj tehnološki giganti resnično počnejo z vašimi podatki? Vir: https://www.dataprotection-officer.com

Ko podjetja prenesejo svoje podatke na podružnice ... ... in vas zavezujejo tudi tretje osebe

Če bi morali prebrati pogoje tehnološkega velikana, to ne bilo dovolj, prebrati bi morali tudi pogoje uporabe tiste druge družbe, ki obdeluje vaše podatke.
Amazon pravi, da lahko svoje podatke delijo s tretjimi osebami, uporabniki pa morajo *"skrbno pregledati svoje izjave o zasebnosti in druge pogoje uporabe"*.
Ali, če uporabljate izdelke **Apple**, se vaši osebni podatki delijo s podjetji, *"ki zagotavljajo storitve, kot so obdelava podatkov, razširitev kredita... in ocenjevanje zanimanja za njihove izdelke in storitve"*.
Splošna uredba o varstvu podatkov (GDPR), ki je začela veljati maja letos, od družb ne zahteva, da navedejo tretje stranke v svojih pogojih.
Ailidh Callander, pravnik pri **Privacy International**, pravi, da ima to zaskrbljujoče posledice: *»To pomeni, da podjetja, kot so posredniki podatkov, lahko uporabljajo vašo lokacijo, vaše interese, vaše stike in še veliko več, da vas profilirajo«*. *"Politike zasebnosti so lahko zelo dolge, vendar je zelo pomembno, da si zanje vzamete čas, da ne pogledamo le to, kateri podatki se zbirajo in zakaj, temveč tudi s kom te podatke delijo (in za kakšne namene)"*, dodaja Callander. Wikipedia po drugi strani ne posreduje vaših osebnih podatkov tretjim osebam za namene trženja.

Tinder zbira podatke o žiroskopu
Včasih zbiranje podatkov presega ime, starost in lokacijo. Tinder pravi, da aplikacija zbira podatke iz merilnika pospeška vašega telefona (za merjenje gibanja), žiroskopov (ki merijo kot, kako držite telefon) in kompasov. Vendar ne povedo zakaj točno, se ti podatki uporabljajo.

Facebook ohranja izbrisana iskanja ...
Facebook ponuja možnost brisanja iskanj iz njihove zgodovine, s čimer uporabniku omogočijo vtis, da so zapisi njihovih iskanj čisti. Težava pa je, da niso. Njihova politika podatkov navaja, da lahko zgodovino iskanja kadar koli izbrišete, *"dnevnik tega iskanja se po 6 mesecih izbriše"*.

Kaj tehnološki giganti resnično počnejo z vašimi podatki? Vir: https://www.dataprotection-officer.com

Facebook vas spremlja, tudi če ste izključili aplikacijo
Facebook celo spremlja, kaj počnete, ko niste prijavljeni - ali če nimate računa. Po svoji podatkovni politiki delujejo z oglaševalci, razvijalci aplikacij in založniki, ki jim lahko pošljejo informacije o svojih dejavnostih izven Facebook-a preko nekaj imen, ki jih imenujemo Facebook Business Tools. Ti partnerji *"zagotovijo informacije o vaših dejavnostih izven Facebook-a, vključno z informacijami o vaši napravi, spletnih mestih, ki jih obiščete, nakupih, ki jih naredite, (in) oglasih, ki jih vidite"*.

LinkedIn skenira vaša zasebna sporočila
Če ste mislili, da so zasebna sporočila zasebna, razmislite znova. LinkedIn uporablja avtomatsko tehnologijo skeniranja sporočil, v skladu s svojo politiko zasebnosti. Družba pravi, da to naredi zato, da bi zagotovila zaščito pred zlonamernimi spletnimi mesti ali neželeno pošto in predlaga samodejne odgovore. Medtem Twitter, shranjuje in obdeluje vaša sporočila. Uporablja podatke o komu ste komunicirali, s kom in kdaj (vendar ne vsebine teh sporočil), da bi bolje razumeli uporabo njihovih storitev, da bi zaščitili varnost in celovitost naše platforme.

Če ste mlajši od 18 let, bi morali vaši starši prebrati to z vami
Applovi pogoji pravijo, da bi morali "otroci, mlajši od določene starosti, pregledati ta sporazum s svojim staršem ali skrbnikom, da bi to lahko razumel otrok in starš ali zakoniti zastopnik. Kljub temu, kot je razvidno iz raziskave BBC, da bi se prebili in prebrali politiko in pogoje glede zasebnosti, bi povprečna odrasla oseba potrebovala več kot 40 minut - kaj šele povprečen 13-letnik. Tudi če ste prebrali pravilnik o zasebnosti, vas Amazon ponovno vabi, da preverite njihovo politiko: *»Naše podjetje se nenehno spreminja in tudi naša obvestila o zasebnosti se bodo spreminjala. Pogosto spremljajte našo spletno stran, da boste seznanjeni z vsemi spremembami«*.

Ne uporabljajte iPhone za izdelavo jedrskega orožja
Apple ima v svojih pogojih uporabe za Veliko Britanijo napisano, zakaj stranke ne smejo uporabljati njihovih izdelkov *"za kakršne koli namene, ki jih prepoveduje zakonodaja Združenih držav Amerike"*. V skladu z njihovo opredelitvijo, to vključuje tudi *"razvoj, načrtovanje ali proizvodnjo jedrskih, raketnih ali kemičnih ali bioloških orožij"*.

PlusPrivacy: Projekt EU za zaščito naše zasebnosti na spletu
Vir: https://www.dataprotection-officer.com

Orodje za varovanje zasebnosti, ki ga financira EU, bo zaščitilo vaše osebne podatke, pomagalo pa vam bo tudi pri njihovi prodaji

Težko je zaščititi zasebnost na spletu, še posebej zato, ker smo bili leta in leta premalo previdni ob uporabi spleta. Večina spletnih storitev omogoča prijavo z našimi obstoječimi računi socialnih omrežij – kar nam prihrani čas in trud – vendar ne brez posledic za zasebnost.

Nova odprta storitev, ki jo je ustvaril projekt OPERANDO https://www.operando.eu/servizi/notizie/notizie_homepage.aspx, bo to poskušala odpraviti s povečanjem moči uporabnikov nad osebnimi podatki, ki jih prenesejo na ponudnike spletnih storitev.

Storitev se imenuje PlusPrivacy https://plusprivacy.com/ in ponuja enotno nadzorno ploščo za zasebnost na družbenih omrežjih, kjer lahko upravljate z nastavitvami zasebnosti za Facebook, Twitter, LinkedIn in druge – vse na enem mestu. Obstaja tudi »zasebnost z enim samim klikom«, ki samodejno nastavi vse vaše račune glede na »vrednote, prijazne do zasebnosti«.

Poleg tega ima PlusPrivacy podobno nadzorno ploščo, preko katere si lahko ogledate zbiranje osebnih podatkov aplikacij in njihovih razširitev, skupaj z alternativno storitvijo e-poštne identitete. To so izjemno pomembna orodja za povečanje ozaveščenosti ljudi o njihovi prisotnosti na spletu. Najbolj zanimiva pa je funkcija »Zasebnost-za-korist« (Privacy for Benefit).

»Zasebnost-za-korist« se še razvija, vendar je načrt ustvariti nove poslovne modele, ki bodo uporabnikom omogočali delno izmenjavo njihovih osebnih podatkov za »ekonomske koristi« – kar bi lahko bil prvi korak k osebnim podatkom kot valuti.

TNW se je obrnil na ekipo PlusPrivacy, da bi vprašal, kako so predvideli te vrste podatkovnih transakcij med potrošniki in podjetji. Upali smo, da bi bile gospodarske koristi morda realen denar, vendar pa načrti PlusPrivacy tega v tem trenutku ne vključujejo.

PlusPrivacy: Projekt EU za zaščito naše zasebnosti na spletu
Vir: https://www.dataprotection-officer.com

Orodje za varovanje zasebnosti, ki ga financira EU, bo zaščitilo vaše osebne podatke, pomagalo pa vam bo tudi pri njihovi prodaji

TNW se je obrnil na ekipo PlusPrivacy, da bi vprašal, kako so predvideli te vrste podatkovnih transakcij med potrošniki in podjetji. Upali smo, da bi bile gospodarske koristi morda realen denar, vendar pa načrti PlusPrivacy tega v tem trenutku ne vključujejo. Običajno bo to pomenilo popust, ki ga bo ponudil ponudnik izdelkov / storitev, je dejal Zeev Pritzker iz Arteevo Technologies Ltd., eden od partnerjev v projektnem konzorciju OPERANDO. PlusPrivacy bo nato dobil majhno pristojbino za posredovanje posla, ki ga bo plačal ponudnik izdelkov / storitev.

Po podatkih podjetja Pritzker bi bili osebni podatki, s katerimi bi trgovali s ponudniki storitev prek storitve PlusPrivacy, enaki kot jih trenutno posredujete pri vsakem vpisu v Facebook, Twitter ali Google račun.

Medtem ko se večina uporabnikov tega ne zaveda, prijava v račune socialnih omrežij tretjim osebam omogoča dostop do njihovih podatkov na družbenem omrežju. PlusPrivacy to preprečuje - namesto tega uporabnika opozarja na prijavo z e-poštnim naslovom in geslom, hkrati pa omogoča uporabniku možnost, da se prijavi na, recimo, Facebook, in prejme neko ekonomsko korist v zameno.

Pritzker poudarja, da se bo izmenjava zgodila samo, če se bodo uporabniki za to izrecno odločili. Cilj PlusPrivacy je, da se potrošniki začnejo zavedati, katere osebne podatke implicitno dajejo, in jim pomagati prevzeti nadzor nad njimi. Storitev, ki jo podpira EU program Horizont 2020, https://ec.europa.eu/programmes/horizon2020/ , bo za navadne smrtnike popolnoma brezplačna, ponudnikom spletnih storitev pa bodo ponujene plačljive storitve.
Še vedno v različici beta storitev še zdaleč ni popolna, a skupina PlusPrivacy hitro odpravlja težave, na katere jih uporabniki opozorijo https://www.reddit.com/r/europrivacy/comments/6u012q/plusprivacy_free_eusponsored_privacy_dashboard/ . Tu se lahko prijavite https://plusprivacy.com/register/ na odprto beta različico in začnete jemati nazaj svojo zasebnost (vsaj dokler je ne začnete prodajati).

Vir: TNW, https://thenextweb.com/security/2017/08/17/eu-funded-online-privacy-tool-will-protect-your-data-and-help-you-sell-it/?amp=1

Obrekovanje !

Iztok Maver
Zaporedna številka potrdila dodatne kvalifikacije
53/2018-1975/3

Nenehno obrekovanje lahko spodkoplje zdravje.

Škodoželjni pogovori in naslajanje nad težavami drugih, ki postajajo čedalje pogostejši v našem vsakdanu, slabšajo kakovost življenja, lahko pa tudi škodujejo vašemu zdravju. Nenehno privoščljivo iskanje in odkrivanje napak posameznikov ter izpostavljanje njihovih pomanjkljivosti, vas bo počasi porinilo v negativne miselne vzorce. Z raziskavami so potrdili, da so pesimistični ljudje bolj nagnjenim k zdravstvenim težavam, kot sta prehlad in razne bolečine. Zato raje opustite obrekovanje, čeprav je 'sočne novice' težko zadržati zase. Počutili se boste bolje, če boste pozitivno naravnani.

Obrekovanje, 159. člen kazenskega zakonika:

(1) Kdor o kom trdi ali raznaša kaj neresničnega, kar lahko škoduje njegovi časti ali dobremu imenu, čeprav ve, da je to, kar trdi ali raznaša, neresnično, se kaznuje z denarno kaznijo ali zaporom do šestih mesecev.
(2) Če je dejanje iz prejšnjega odstavka storjeno s tiskom, po radiu, televiziji ali z drugim sredstvom javnega obveščanja ali na spletnih straneh ali na javnem shodu, se storilec kaznuje z denarno kaznijo ali zaporom do enega leta.
(3) Če je tisto, kar se neresnično trdi ali raznaša, take narave, da ima hude posledice za oškodovanca, se storilec kaznuje z zaporom do dveh let.

Nepooblaščen vpogled !

Kontrola nepooblaščenih vpogledov na podlagi revizijskih sledi

Vsi podatki, tako osebni podatki, kot posebni ali občutljivi osebni podatki, ki jih upravljalec obdeluje, so predmet sledenja preko revizijskih sledi, ki se hranijo kot log datoteke v informacijskem sistemu. Te revizijske sledi se bodo pregledovale nenapovedano 1x do 2x letno. Upravljavec bo na podlagi poročil povabil na zagovor zaposlene, za katere bo ugotovil sum nepooblaščenih vpogledov v osebne ali posebne osebne podatke, oziroma bo ravnal skladno z zakonom. Kot nepooblaščen vpogled se lahko smatra že vpogled v rojstne podatke osebe z namenom čestitke za rojstni dan zato predlagam, da take podatke dobite osebno, preko razgovora z dotično osebo.

Zloraba osebnih podatkov, 143. člen kazenskega zakonika

(1) Kdor brez podlage v zakonu ali v osebni privolitvi posameznika, na katerega se osebni podatki nanašajo, osebne podatke, ki se obdelujejo na podlagi zakona ali osebne privolitve posameznika, posreduje v javno objavo ali jih javno objavi, se kaznuje z denarno kaznijo ali zaporom do enega leta.
(2) Enako se kaznuje, kdor vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.
(5) Kdor stori dejanje iz prvega odstavka tega člena tako, da posreduje v javno objavo ali javno objavi občutljive osebne podatke, se kaznuje z zaporom do dveh let.
(6) Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do petih let.
(7) Pregon iz četrtega odstavka tega člena se začne na predlog.

Grožnja z razkrivanjem

Kako ravnati pri grožnji z razkrivanjem vaših občutljivih osebnih podatkov

Zadnje čase se pojavlja trend groženj z razkrivanjem vaših osebnih podatkov. Naj vas panika ne zagrabi.
Zamenjajte vsa gesla, shranite vse podatke in ignorirajte grozilno pismo.

Dejanski primer grozilne e-pošte:

Sent: Thursday, October 18, 2018 1:25 PM
To: Ime priimek
Subject: ime.priimek@primer.si is hacked

Hello!

My nickname in darknet is hamil58.
I hacked this mailbox more than six months ago, through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

So, your password from ime.priimek@primer.si is xixyfafi

Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

Grožnja z razkrivanjem

Dejanski primer grozilne e-pošte, nadaljevanje:

I was most struck by the intimate content sites that you occasionally visit.
You have a very wild imagination, I tell you!

During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.
Oh my god! You are so funny and excited!

I think that you do not want all your contacts to get these files, right?
If you are of the same opinion, then I think that $852 is quite a fair price to destroy the dirt I created.

Send the above amount on my BTC wallet (bitcoin): 1EZS92K4xJbymDLwG4F7PNF5idPE62e9XY
As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.

Otherwise, these files and history of visiting sites will get all your contacts from your device.
Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!
Since reading this letter you have 48 hours!
After your reading this message, I'll receive an automatic notification that you have seen the letter.
I hope I taught you a good lesson.
Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!
Good luck!

Problematika je opisana tudi na : https://www.varninainternetu.si/izsiljevanje-z-domnevno-okuzbo-racunalnika/

Odgovori na vprašanja

Fotografiranje:

https://www.rtvslo.si/slovenija/ali-lahko-fotografiramo-svojega-otroka-v-druzbi-sosolcev-in-to-objavimo-na-druzbenih-omrezjih/477454

Aplikacije za zaščito telefona:

https://www.racunalniske-novice.com/novice/mobilna-telefonija/dogodki-in-obvestila/10-najboljsih-aplikacij-za-zascito-androida.html?RSSe4c936a9189ce08942341d127a2787dd