Úvod do kybernetické bezpečnosti

Martin Hájek

Jak to celé začalo?

Národní úřad pro kybernetickou a informační bezpečnost

2011	NBÚ ustanoven jako gestor KB Národní centrum kybernetické bezpečnosti
2012	Národní strategie kybernetické bezpečnosti I.
2015	Zákon o kybernetické bezpečnosti Národní strategie kybernetické bezpečnosti II.
2016	Směrnice NIS
2017	Novela zákona NÚKIB

NBÚ

nckb

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Činnost NÚKIB

- provozování Vládního CERT České republiky,
- příprava legislativy a bezpečnostních standardů,
- ochrana utajovaných informací,
- kryptografická ochrana,
- cvičení kybernetické bezpečnosti,
- osvěta a podpora vzdělávání,
- výzkum a vývoj.

Vládní CERT (GovCERT.CZ) a týmy typu CSIRT hrají klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů podle zákona o kybernetické bezpečnosti (181/2014 Sb.) a jeho prováděcích předpisů.

- Koordinační činnost a pomoc při řešení incidentů,
- Projekt systém detekce,
- Penetrační testování,
- Forenzní laboratoř,
- Kybernetická bezpečnost operačních technologií,
- Vzdělávání a výzkumná činnost.

Směrnice Evropského parlamentu a Rady (EU)

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

Hlavní cíle směrnice NIS

- Ujednotit právní úpravu členských států v oblasti bezpečnosti sítí a informačních systémů
- Zavést jednotný standard úrovně kybernetické bezpečnosti s ohledem na lepší fungování vnitřního trhu.
- U nás některé její části upravuje Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

- Zákon upravuje práva a povinnosti a působnost a pravomoci orgánů veřejné moci
- v oblasti kybernetické bezpečnosti. V platnosti od 29. srpna 2014.

Hlavní cíle zákona jsou:

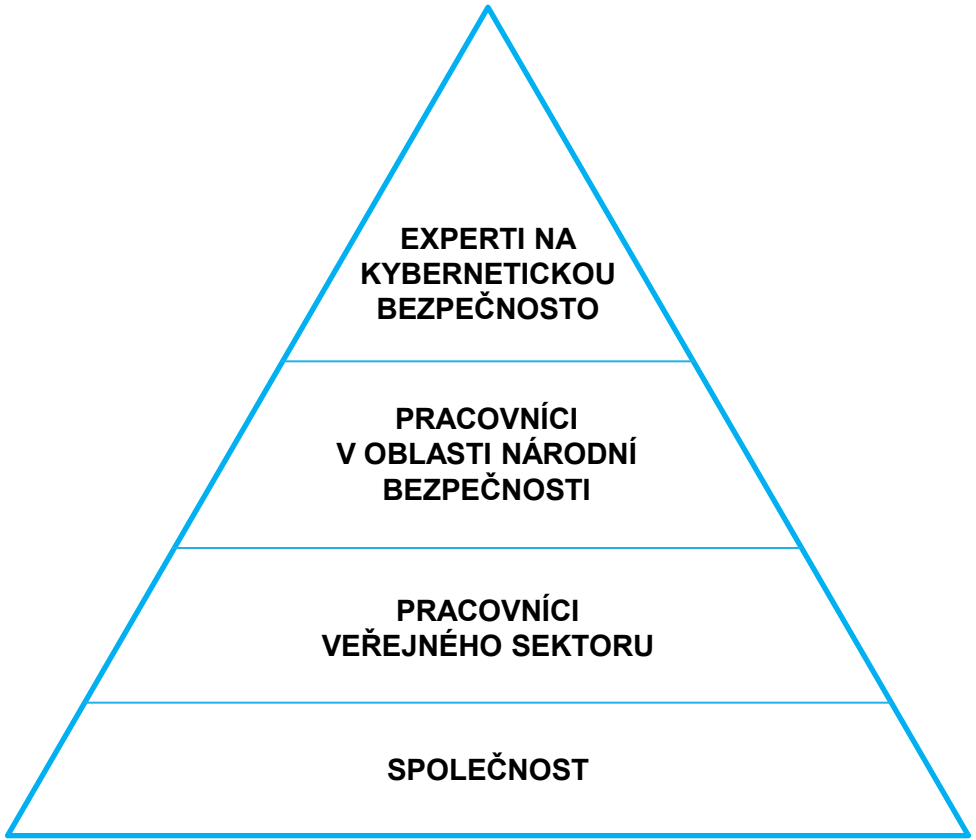
- určit základní úroveň bezpečnostních opatření
- zlepšit detekci kybernetických bezpečnostních incidentů v ČR
- zavést hlášení kybernetických bezpečnostních incidentů
- zavést systém opatření k reakci na kybernetické bezpečnostní incidenty
- upravit činnost dohledových pracovišť

Kritická informační infrastruktura

- **Kritickou informační infrastrukturou (KII)** se dle § 2 písm. g) a písm. i) zákona č. 240/2000 Sb., krizového zákona, rozumí prvek nebo systém prvků kritické infrastruktury, v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti dle § 2 písm. b) zákona č. 181/2014 Sb. o kybernetické bezpečnosti.

- Obecně se jedná o systémy a služby, jejichž nefunkčnost nebo špatná funkčnost by měla závažný dopad na bezpečnost státu, jeho ekonomiku, veřejnou správu a v důsledku na zabezpečení základních životních potřeb obyvatelstva.

Odolný systém zajištění kybernetické bezpečnosti



Zdroj: Národní strategie kybernetické bezpečnosti České republiky 2020 – 2025, str.19

Proč je osvěta potřebná?

OSTATNÍ DŮVODY:
- zero day, phishing, backdoor...

LIDSKÁ CHYBA:
- špatná konfigurace systému
- neaktualizované aplikace
- použití defaultních přihlašovacích údajů
- použití slabých hesel
- ztracené notebooky a telefony
- vyzrazení citlivých informací skrze chybné emailové adresy

Za rok **2024 celkem 268 incidentů**. Největší podíl **DDoS útoky**.

Podíl **ransomware jen 11 %**, ale z hlediska dopadu jde o závažnou hrozbu.

Kdo za co odpovídá?

Existují zde dvě úrovně:

- **odborníci (správci IT a role odpovědné za bezpečnost),**
- **uživatelé, kteří technologie využívají.**

Zodpovědnost za přístup k počítači, tedy i k heslům, je na každém uživateli zvlášť. Stejně tak je na jednotlivcích i to, jestli dodržují zásady archivace, zálohování a další bezpečnostní předpisy.

V oblasti kybernetické kriminality i bezpečnosti hraje roli zejména to, že **jednotlivci nevnímají virtuální svět jako součást reality a nepoužívají podvědomé bezpečnostní mechanizmy**.

Patří mezi ně návyky typu:

- „nebavím se s cizími lidmi“,
- „své heslo nikomu nesděluji“,
- „moje fotografie nejsou věc veřejná“
- a další věci, které nás odmala učili.

ZÁKLADNÍ BEZPEČNOSTNÍ POJMY A DOPORUČENÍ

Kybernetický prostor

Definice ze zákona

kybernetickým prostorem se rozumí soubor sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě

Kybernetický prostor tvoří:
- Internet
- Stolní počítače
- Notebooky
- Mobilní zařízení a tablety
- Internet věcí
- Chytré hodinky, náramky

V podstatě vše, co může předávat informace.

Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.

PRAVIDLA, OPATŘENÍ A PROSTŘEDKY

PRO OCHRANU UŽIVATELŮ A SYSTÉMU

Obecné zásady bezpečnosti

Bezpečnostní politika IT:
Pravidla, směrnice a praktiky, které rozhodují o tom, jak jsou aktiva včetně citlivých informací spravovány, chráněny a distribuovány uvnitř organizace a jejich systémů ICT.

Stanovuje ji architekt kybernetické bezpečnosti.

Schvaluje ji manažer kybernetické bezpečnosti, který dohlíží na její dodržování.

Důležitou roli hraje nezávislý auditor, který kontroluje správné nastavení zásad.

CIA triáda bezpečnosti

Ochrana důvěrnosti, integrity a dostupnosti informací v síti Internet.

DŮVĚRNOST – k informaci nemá přístup nikdo nepovolaný
Vlastnost, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.

INTEGRITA – informace je kompletní tak jak ji zamýšlel autor
Vlastnost přesnosti a úplnosti informace.

DOSTUPNOST – informace je dostupná tehdy, když dostupná být má
Vlastnost přístupnosti a použitelnosti na žádost oprávněné entity.

Ztráta kterékoliv z těchto vlastností je důvodem k nahlášení incidentu osobě, pověřené péčí o IT nebo přímo bezpečnostnímu manažerovi.

HROZBA X UDÁLOST X INCIDENT

HROZBA – něco, co může ohrozit uživatele nebo systém
Je to jakákoliv potenciální okolnost, událost nebo jednání, které mohou být příčinou kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, a která mohou poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby.

KYBERNETICKÁ BEZPEČNOSTNÍ UDÁLOST – Jakákoli událost, která ohrožuje bezpečnost informačních systémů nebo dat.
Kybernetickou bezpečnostní událostí je událost, která může vyústit v kybernetický bezpečnostní incident.

KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT – něco, co se už stalo a je třeba to řešit
Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v kybernetickém prostoru.

Co je to vlastně hacking?

HACKING

- Získání neoprávněného přístupu do systému / služby / počítače.
- Cílená změna běžného fungování počítače/systému za pomocí skriptů a speciálních programů.
- Cílem bývá získávání informací a manipulace s daty.

PŘÍKLADY

- přístup do cizí e-mailové schránky
- přístup do cizího počítače
- čtení cizích zpráv

Kdo je to ten hacker?

WHITE-HAT HACKER

Počítačový odborník nebo programátor, který má detailní znalosti fungování systému a tyto své znalosti využívá k ochraně systému a uživatelů.

BLACK-HAT HACKER

Počítačový odborník, který své znalosti využívá k napadení/narušení fungování systému nebo získávání a poškozování dat. Provádí nezákonnou činnost.

GREY-HAT HACKER

Odborník, který získává přístup do systému i bez povolení vlastníka, ale nikdy by záměrně nepoškodil systém, do kterého se dostal a neukradl by peníze. Dost často o svém úspěšném vniknutí upozorní administrátory.

Národní úřad
pro kybernetickou
a informační bezpečnost

JAK NA SILNÉ HESLO

Silné heslo

- Bezpečné heslo má mít nejméně 12 znaků.
- Má obsahovat kombinaci malých a velkých písmen, číslic a ideálně speciální znaky.
- Musí být dostatečně složité, ale zapamatovatelné.
- musí být dostatečně často měněno. Ideální interval je určen nařízením seshora, ale heslo měníme vždy, když máme podezření na únik hesla stávajícího.

Kombinace slov nebo písmen ze známé říkanky, písničky nebo atypické věty spolu s doplněním číslic je ideální pomůckou pro tvorbu hesel.

Jak na správné heslo...

VELITELSTVÍ KYBERNETICKÝCH A INFORMAČNÍCH SIL

Zadejte nové heslo:

Heslo musí obsahovat více než 8 znaků.

Heslo musí obsahovat alespoň jednu číslici.

Heslo nesmí obsahovat diakritiku.

Heslo nesmí obsahovat mezery.

Heslo musí obsahovat alespoň jedno velké písmeno.

Heslo nesmí obsahovat více velkých písmen po sobě.

Heslo nesmí obsahovat interpunkci.

Heslo musí obsahovat jeden speciální znak.

granát

ruční granát

2 ruční granáty

2 rucni granaty

2blbyrucnigranaty

2BLBYrucnigranaty

2BlbyRucniGranaty,UzMiKonecneDejteTenPristup

2BlbyRucniGranatyUzMiKonecneDejteTenBlbejPristup

TakTedJsemSeUzFaktNasral2BlbyRucniGranatyUzMiKonecneDejteTenBlbejPristup!

Omlouváme se, ale toto heslo již bohužel někdo používá. Vymyslete jiné.

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

Heslo

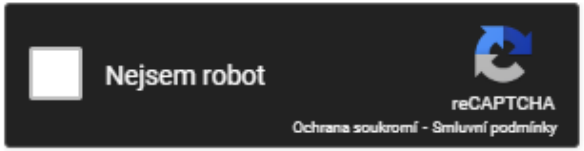
Generate →

Your String	Heslo
MD5 Hash	3ea4db050dfd4daa3a93e9434c468776 Copy
SHA1 Hash	894f36e5fe639267301de83d341819acc0a14d4b Copy

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
3ea4db050dfd4daa3a93e9434c468776
```



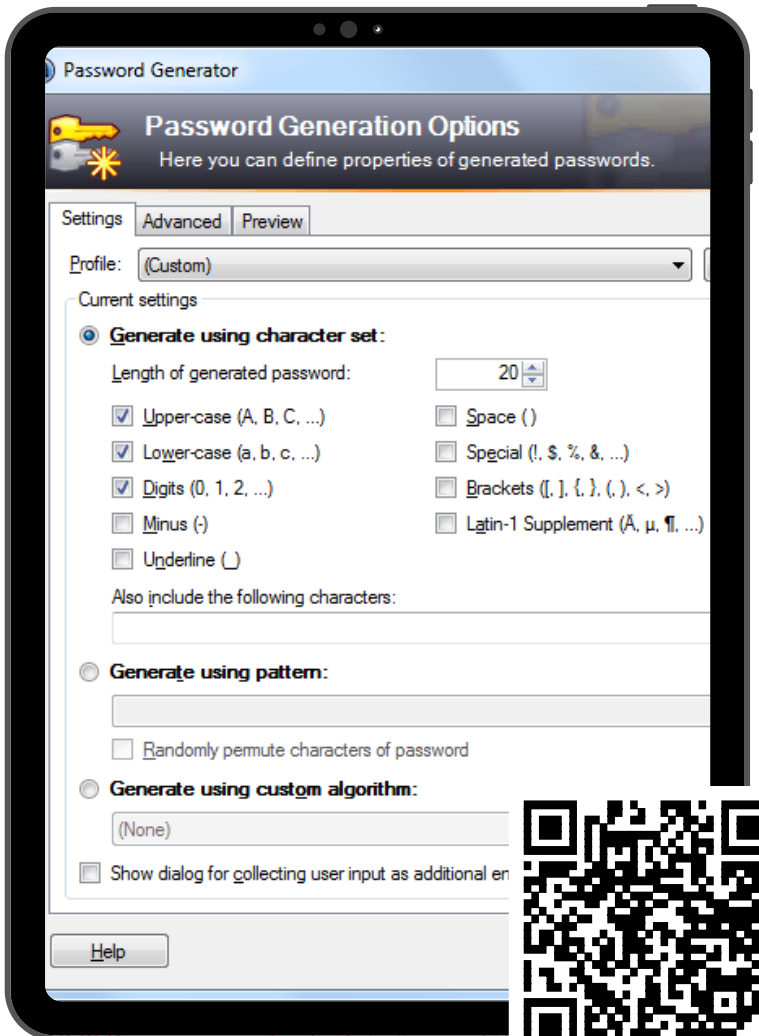
Crack Hashes

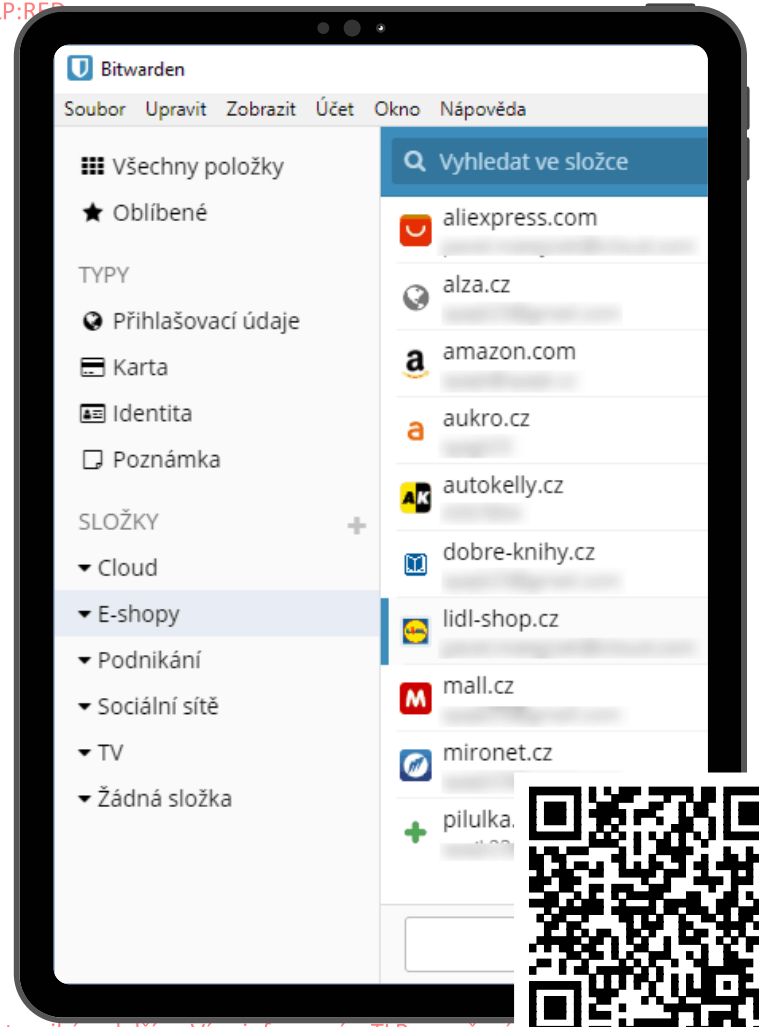
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
3ea4db050dfd4daa3a93e9434c468776	md5	Heslo

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist


Password Generator
Password Generation Options
Here you can define properties of generated passwords.
Settings
Advanced
Preview
Profile:
(Custom)
Current settings
Generate using character set:
Length of generated password:
20
Upper-case (A, B, C, ...)
Lower-case (a, b, c, ...)
Digits (0, 1, 2, ...)
Minus (-)
Underline (_)
Space ( )
Special (!, $, %, &, ...)
Brackets ([,], {, }, (,), <, >)
Latin-1 Supplement (Ä, µ, ¶, ...)
Also include the following characters:
Generate using pattern:
Randomly permute characters of password
Generate using custom algorithm:
(None)
Show dialog for collecting user input as additional en
Help


Bitwarden
Soubor
Upravit
Zobrazit
Účet
Okno
Nápověda
Všechny položky
Oblíbené
TYPY
Přihlašovací údaje
Karta
Identita
Poznámka
SLOŽKY
Cloud
E-shopy
Podnikání
Sociální sítě
TV
Žádná složka
Vyhledat ve složce
aliexpress.com
alza.cz
amazon.com
aukro.cz
autokelly.cz
dobre-knihy.cz
lidl-shop.cz
mall.cz
mironet.cz
pilulka.

Multifaktorové ověřování

Po přihlášení prostřednictvím uživatelského jména a hesla je vyžadován ještě další krok k ověření identity. Využívá se pro významné služby, systémy a účty.

Pomůže v případě, že by se k heslu dostal někdo cizí a chtěl ho zneužít.

Nejčastěji bývá realizováno prostřednictvím:
SMS případně e-mail
Mobilní aplikace
Token (čipová karta,…)

Zacházení s daty - zálohování

- Zálohování není upraveno závazným předpisem, ale je nezbytné
- pro zajištění chodu organizace v případě náhlého výpadku informačních systémů.
- Záloha musí být uchována odděleně od pořizovacího zařízení.
- Musí být udržována v čitelné podobě.
- Pořízení záloh lze nastavit automaticky na dobu, kdy neomezí provoz daného systému.
- Zálohy musí být vždy šifrované a uložené na bezpečném místě
- Ideálně jsou chráněny i před vnějšími vlivy.

SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství

Nemusí být vůbec zaměřeno přímo na nás. Děje se plošně například díky úniku telefonních čísel nebo e-mailů z databází.

„Dobrý den, někdo se snaží dostat do vašeho účtu. Pokud tomu chceme zabránit, potřebuji vaše heslo do internetového bankovnictví kvůli ověření.“

„Vidíme u vašeho účtu nedoplatek za služby ve výši 2150,- po splatnosti. Pokud nechcete, aby vám byla služba odpojena, pošlete doplatek v plné výši na naše speciální konto: XXXXXX/XXXX a vše bude v pořádku.“

Sociální inženýrství – doporučení

- Poučte se z cizích (případně vlastních) chyb.
- Důvěřuj, ale prověřuj.
- Nenechte se zastrašit.
- Neunáhlujte se.
- Nebuďte zbytečně zvědaví.
- Nebuďte zbytečně sdílní.
- Nestyďte se reportovat.
- Pamatujte, že nikdo vám nic nedá zadarmo

Phishing

- Podvodná technika využívající informační a komunikační technologie k získávání citlivých údajů
- Zpravidla je v prvotní fázi celého podvodu užito sociální inženýrství.

Cílem je získat například:

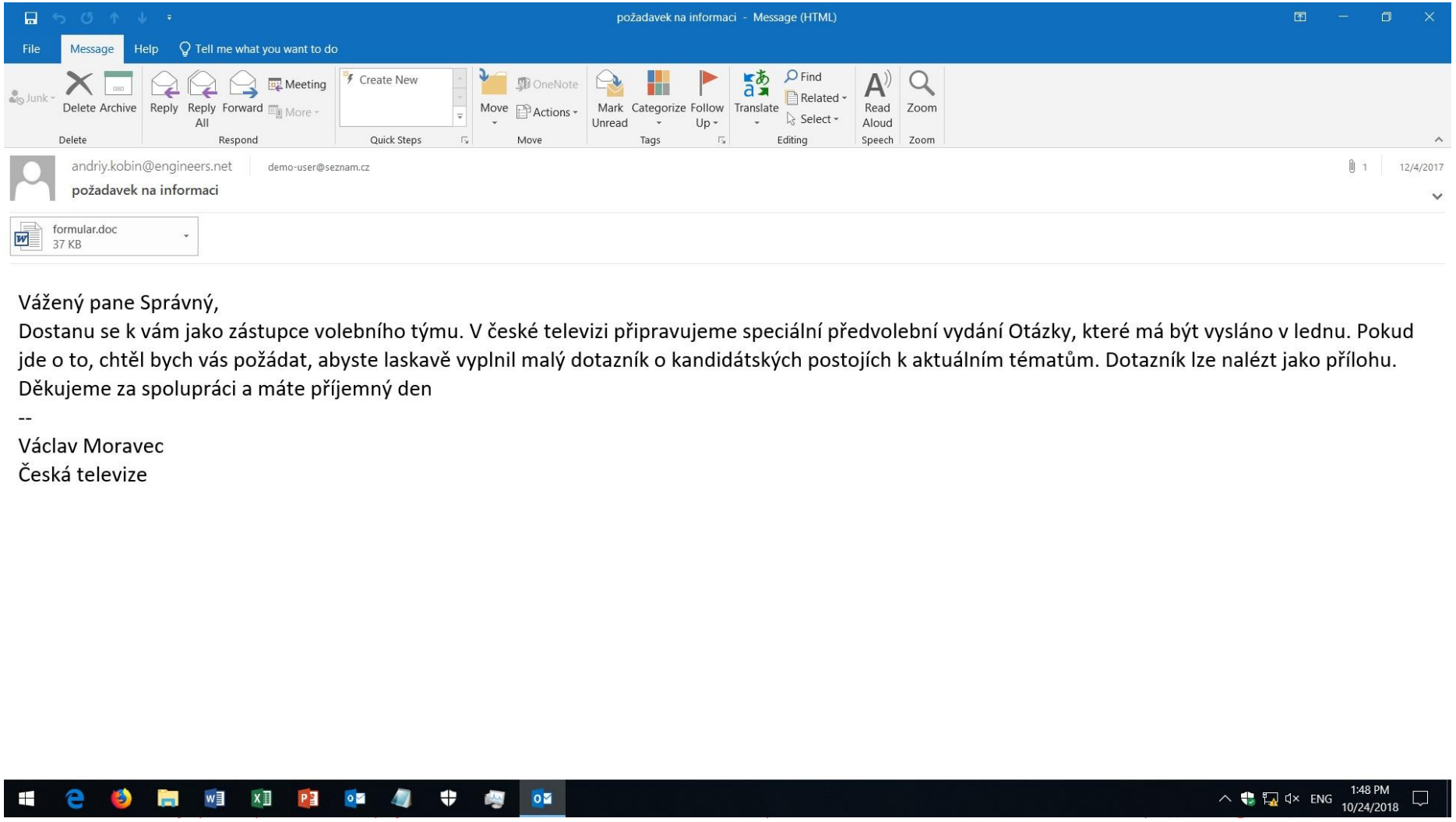
- přihlašovací údaje k různým webovým službám, účtům a aplikacím, uživatelská hesla, čísla platebních karet apod.

Rozpoznávání phishingu

Důležité je být ve střehu a nebezpečí phishingu nepodceňovat.

- Krkolomná čeština, gramatické chyby,
- Neznámá adresa odesílatele,
- Podezřele vyhlížející adresa odesílatele – př. **balicky@p0sta.gi.cz**
- Neznámé přílohy, které nečekáme.
- Podezřele vypadající odkazy

  http://yssqwscscqscqscqc.ownip.net/71552du64781748ix86181lm202482cj12522dw26864rr#sofkvqjhddtlesbmwwhrfkoopadlwqeskmzualdrccoqeshkua
- Časová tíseň. Teď je potřeba něco udělat!


požadavek na informaci - Message (HTML)
File
Message
Help
Tell me what you want to do
Junk
Delete
Archive
Reply
Reply All
Forward
Meeting
More
Delete
Respond
Create New
Quick Steps
Move
OneNote
Actions
Move
Mark Unread
Categorize
Follow Up
Tags
Translate
Find
Related
Select
Editing
Read Aloud
Speech
Zoom
Zoom
andriy.kobin@engineers.net
demo-user@seznam.cz
1
12/4/2017
požadavek na informaci
formular.doc
37 KB
Vážený pane Správný,
Dostanu se k vám jako zástupce volebního týmu. V české televizi připravujeme speciální předvolební vydání Otázky, které má být vysláno v lednu. Pokud jde o to, chtěl bych vás požádat, abyste laskavě vyplnil malý dotazník o kandidátských postojích k aktuálním tématům. Dotazník lze nalézt jako přílohu.
Děkujeme za spolupráci a máte příjemný den
--
Václav Moravec
Česká televize
ENG
1:48 PM
10/24/2018

informace pro ČT - Message (HTML)

File | Message | Help | Tell me what you want to do

Junk | Delete | Archive | Reply | Reply All | Forward | Meeting | More | Create New | Move | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Read Aloud | Zoom

Delete | Respond | Quick Steps | Move | Tags | Editing | Speech | Zoom

Václav Moravec <andriy.kobin@engineers.net> demo-user@seznam.cz 1 12/4/2017

informace pro ČT

formular.doc
37 KB

Dobrý den, pane Správný,
obracím se na Vás jako zástupce volebního týmu. V České televizi právě připravujeme předvolební speciál Otázek, který se objeví ve vysílání v polovině ledna. V této souvislosti Vás chci požádat a vyplnění krátkého dotazníku o postojích vašeho kandidáta k aktuálním tématům. Dotazník naleznete v příloze.
Děkuji za Vaši ochotu a přeji hezký den

--

Václav Moravec
MODERÁTOR, REDAKTOR
Česká televize

ENG 1:50 PM 10/24/2018

informace pro ČT - Message (HTML)

File | Message | Help | Tell me what you want to do

Junk | Delete | Archive | Reply | Reply All | Forward | Meeting | More | Create New | Move | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Read Aloud | Zoom

Delete | Respond | Quick Steps | Move | Tags | Editing | Speech | Zoom

Václav Moravec <vaclav.moravec@ceskaletevize.cz> demo-user@seznam.cz 1 12/4/2017

informace pro ČT

formular.doc
37 KB

Dobrý den, pane Správný,
obracím se na Vás jako zástupce volebního týmu. V České televizi právě připravujeme předvolební speciál Otázek, který se objeví ve vysílání v polovině ledna. V této souvislosti Vás chci požádat a vyplnění krátkého dotazníku o postojích vašeho kandidáta k aktuálním tématům. Dotazník naleznete v příloze.
Děkuji za Vaši ochotu a přeji hezký den

--

Václav Moravec
MODERÁTOR, REDAKTOR
Česká televize

ENG 1:51 PM 10/24/2018

informace pro ČT - Message (HTML)

File | Message | Help | Tell me what you want to do

Junk | Delete | Archive | Reply | Reply All | Forward | Meeting | More | Create New | Move | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Read Aloud | Zoom

Delete | Respond | Quick Steps | Move | Tags | Editing | Speech | Zoom

Václav Moravec <vaclav.moravec@ceskatelevize.cz> demo-user@seznam.cz 1 12/4/2017

informace pro ČT

formular.doc
37 KB

Dobrý den, pane Správný,
obracím se na Vás jako zástupce volebního týmu. V České televizi právě připravujeme předvolební speciál Otázek, který se objeví ve vysílání v polovině ledna. V této souvislosti Vás chci požádat a vyplnění krátkého dotazníku o postojích vašeho kandidáta k aktuálním tématům. Dotazník naleznete v příloze.
Děkuji za Vaši ochotu a přeji hezký den

--

Václav Moravec
MODERÁTOR, REDAKTOR
Česká televize

ENG 1:52 PM 10/24/2018

informace pro ČT - Message (HTML)

File | Message | Help | Tell me what you want to do

Junk | Delete | Archive | Reply | Reply All | Forward | Meeting | More | Create New | Move | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Read Aloud | Zoom

Delete | Respond | Quick Steps | Move | Tags | Editing | Speech | Zoom

Václav Moravec <vaclav.moravec@ceskatelevize.cz> demo-user@seznam.cz

1 12/4/2017

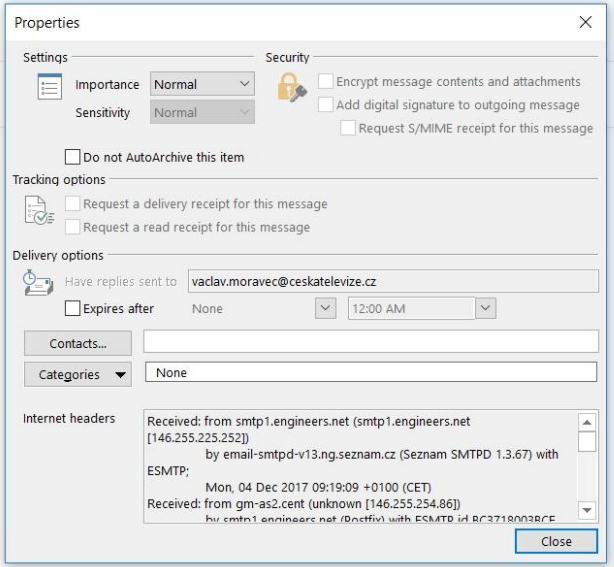
informace pro ČT

formular.doc
37 KB

Dobrý den, pane Správný,
obracím se na Vás jako zástupce volebního týmu. V České televizi právě připravujeme předvolební speciál Otázek, který se objeví ve vysílání v polovině ledna. V této souvislosti Vás chci požádat a vyplnění krátkého dotazníku o postojích vašeho kandidáta k aktuálním tématům. Dotazník naleznete v příloze.
Děkuji za Vaši ochotu a přeji hezký den

--

Václav Moravec
MODERÁTOR, REDAKTOR
Česká televize



ENG 1:53 PM 10/24/2018

Doporučení pro e-mailovou komunikaci

- Bezpodmínečně oddělujeme pracovní a soukromou komunikaci.
- Vždy máme více mailových adres.
- Nepropagujeme cizí mailové adresy – využíváme skryté kopie.
- Pokud se chceme někam jednorázově zaregistrovat, využijeme desetiminutový e-mail.
- Neotevíráme nevyžádanou poštu.
- Neprohlížíme nevyžádané přílohy.

- Nejčastější napadení počítače je právě přes e-mailovou schránku.

Vishing

- Jedna z technik sociálního inženýrství, která je na vzestupu.
- Využívá telefonické hovory k vylákání informací z oběti.
- Může být provedena například přímo útočníkem, volacím automatem nebo i umělou inteligencí.
- Útočník se maskuje například jako klientská podpora IT oddělení a informuje uživatele, že je nutné, aby provedl ověření svého účtu. Útočníci umí navodit dojem důvěryhodného callcentra a navzájem si nás předávat.

Vishing - příběh

Dobrý den, vážená paní Novotná,
tímto Vás zdraví oddělení bezpečnosti První České finanční.
Dne 15.01.2025 jsme s Vámi navázali komunikaci po dobu řešení dané problematiky.

Důvod komunikace: Zpronevěření osobních údajů a přístup třetí strany k Vašemu účtu.

Způsob komunikace: Telefonicky.

V danou chvíli bude prováděn proces aktivace elektronického účtu.

Váš manažer: Karel Svoboda

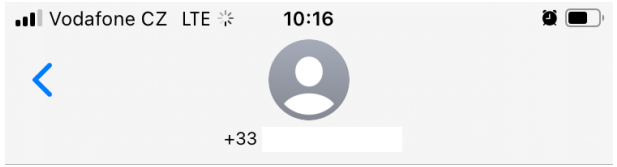
Prosíme Vás o dodržení bankovního tajemství dle smluvních podmínek
a uposlechnutí instrukcí Vašeho manažera.

Přejeme příjemný den.
Vaše První Česká finanční

SMishing

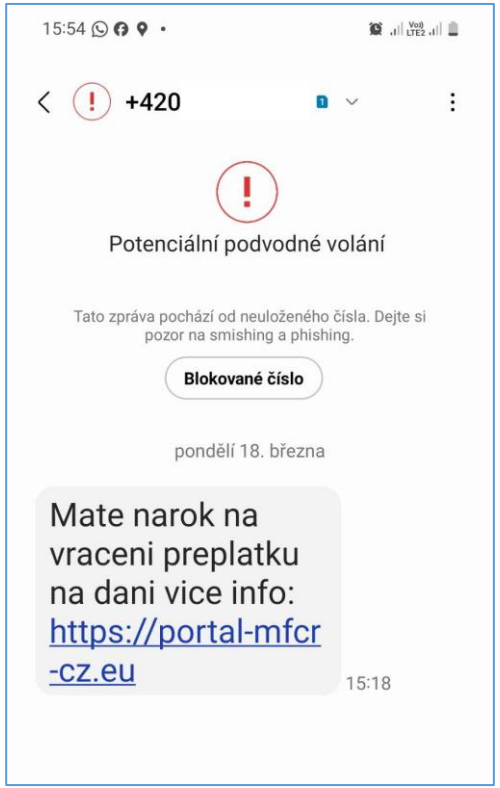
- Zasílání falešných SMS zpráv, které se vydávají za věrohodné sdělení některé existující instituce. Jde o další formu phishingu.
- Útočníci opět využívají techniky sociálního inženýrství.
- Útočníci využívají časovou tíseň.
- Součástí zprávy bývá velice často odkaz směřující na falešnou webovou stránku.
- Cílem je získat od uživatele citlivé údaje, přihlašovací údaje, čísla platebních karet, peníze nebo jej přesvědčit k instalaci škodlivého softwaru do jeho zařízení.
- Zpráva obvykle obsahuje gramatické chyby.
- Součástí také bývá odkaz na neznámé webové stránky.

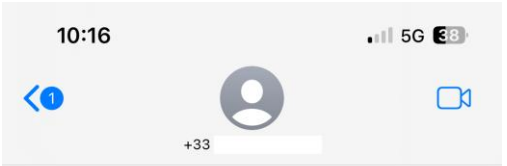
AKTUÁLNĚ – SMiShing



Text Message
Sat 25. 3. at 00:33

ČeskáPošta : Váš balíček čeká na odeslání. Potvrďte prosím své dodací údaje: postaczceska.com
S pozdravem.





Textová zpráva
st 13. 9. 21:40

UPS: Váš balíček F85896565220 bude podléhat dodatečným celním poplatkům. Aktualizujte doručení svého balíku prostřednictvím: https://paketovaktualizacia.com

Baiting

- Technika sociálního inženýrství, která cílí na zvědavost uživatelů.
- Velmi často ve formě „nastražených USB flashdisků“.
- Tyto flashdisky mohou obsahovat škodlivý kód, který se spustí po připojení k počítači a může způsobit celou řadu problémů.
- Útočník může flashdisk nastavit tak, aby se spustil ihned po připojení k počítači bez nutnosti, aby jej spustil uživatel.
- Podle průzkumů takto označenou „flešku“ připojí dva z pěti zaměstnanců.

Nebezpečné USB zařízení může…

- spustit škodlivý kód a infikovat zařízení / celou síť
- umožnit útočníkovi přístup do systému
- ukládat a odesílat komunikaci, stisknuté klávesy, zprávy, atd…
- přesměrovat komunikaci přes škodlivé servery
- zničit zařízení ke kterému bylo připojeno (USB killer)
- nahrávat audio i video v místnosti a odesílat

Antivirová pračka

- Starý počítač/notebook/
- Operační jiný než Windows – například Linux, android, IOS
- Nejvíce útoků a škodlivého kódu je pro operační systém Windows
- Nepřipojen k síti internet /vnitřní síti instituce (pod správou IT)
- Běží na něm aktualizovaný antivirový program
- V případě jeho poškození může být nahrazen jiným „starým zařízením“
- V pracovním prostředí ideálně 1 zařízení na sekci/patro/chodbu.

Vybrané incidenty

Nemocnice Bohunice

Kdy:

- 13. 3. 2020

Co se stalo

- Malware Defray zašifroval data a zničil zálohy
- Vyřazeny klíčové IT systémy a ochromená nemocnice
- Ztracena data z mnohaletého výzkumu z mnoha lékařských oblastí

Doba vyřešení útoku

- Některé části infrastruktury se obnovují i v současné době

Celkové náklady

- proinvestováno přes 300 milionů korun

Centrum pro regionální rozvoj

Kdy:

- prosinec 2021

Co se stalo

- Ransomware zašifroval data na serverech -> byla nutná obnova
- Díky dobrému zálohován ztracena data jen za cca 14 dní
- Vyřazení interních systémů, nešlo také například komunikovat přes e-mail

Doba vyřešení útoku

- Více než rok

Celkové náklady

- Několik milionů korun

Magistrát města Olomouc

Kdy:

- 6. 4. 2022 zašifrována data -> útočníci požadovali výkupné
- 26. 3. 2022 opakovaný útok doplněný o DDoS útok

Co se stalo

- Ransomware napadl více než polovinu počítačů a notebooků se vzdáleným přístupem
- Ochromení využívaných IT systémů a služeb -> návrat k tužce a papíru
- Ukradená a zašifrována data za 1 den

Doba vyřešení útoku

- Více než 14 dní

Celkové náklady

- Několik milionů korun

Ústav jaderného výzkumu

Kdy:

- Prosinec 2022

Co se stalo

- Ransomware zašifroval data na serverech
- Útok na ekonomický úsek ÚJV Řež → výpadek ekonomického systému → pomalé generování výplat
- ÚJV nezaplatil výkupné → útočníci zveřejnili získaná data na internetu
- Útok neohrozil fungování experimentálních reaktorů

Doba vyřešení útoku

- Několik měsíců

Útoků na klienty českých bank přibylo. Škody dosahují stovek milionů korun

Národní úřad pro kybernetickou a informační bezpečnost

Lenka Z
+ sledov

5. 9. 2024, 9:26

Zvýšený poč
zaznamenal
srovnání jde
tohoto roku

Nebezpečný dropper se maskuje za multimediální přehrávač

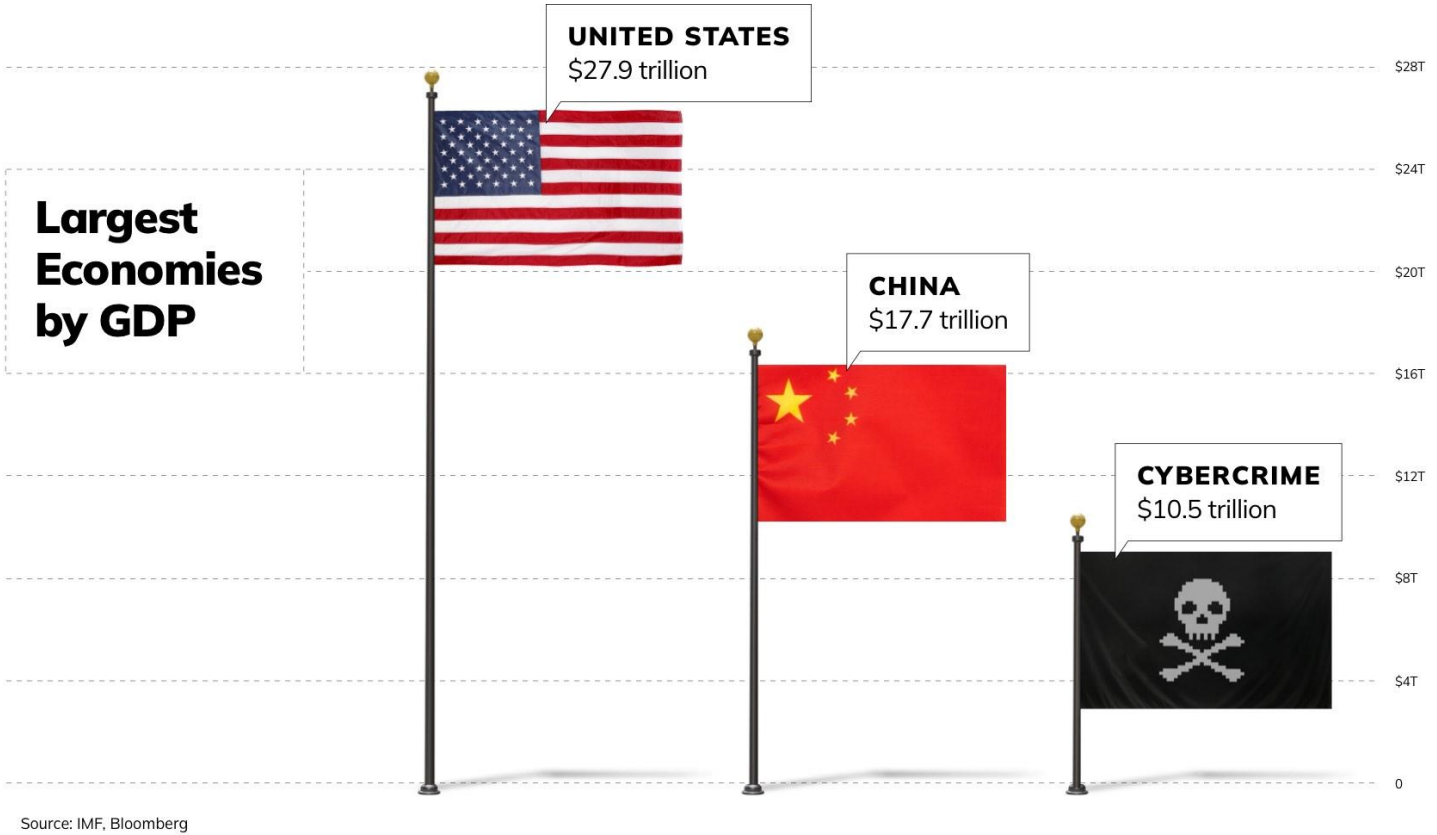
Lenka Zoulová
+ sledovat 108

1

30. 8. 2024, 15:31

Bezpečnostní experti z antivirové společnosti Eset varovali před

Kyberzločin jako ekonomika



Národní úřad
pro kybernetickou
a informační bezpečnost

KYBERNETICKÁ BEZPEČNOST NA CESTÁCH

Před cestou 1/2

- **Nesdílejte informaci o tom, že někam cestujete –** nesdílejte datum a čas cesty, způsob dopravy, čísla letů, autobusů
- **Aktualizujte software** – ujisti se, že operační systém, aplikace i antivirový program jsou aktuální.
- **Zálohujte data** – vytvoř zálohu důležitých souborů na externí disk nebo do zabezpečeného cloudu.
- **Nastavte a používejte silná hesla** – změň slabá hesla a aktivuj dvoufaktorové ověření (2FA) u důležitých účtů.
- **Zkontrolujte oprávnění aplikací** – odeber přístup k poloze, mikrofonu a kameře tam, kde to není nutné.

Před cestou 2/2

- **Vypni automatické připojení k Wi-Fi** – zabráníš tak připojení k nebezpečným sítím, které mohou být podvrhnuté.
- **Nainstaluj a využívejte VPN** – pro bezpečné připojení k internetu na veřejných sítích při cestách.
- **Odebírejte metadata z fotografií** – zejména GPS souřadnice, pokud plánuješ sdílet fotky online.
- **Používejte unikátní účty i prohlížeče pro každou činnost** – v jiném prohlížeči si čtěte e-maily a v jiném nakupujte například lístky, aby nedošlo ke zneužití cookies, které jsou sdílené.
- **Informujte blízké** – sdílej plán cesty jen s důvěryhodnými osobami, ne veřejně.

V rámci cesty

- **Nepřihlašujte se do citlivých služeb** – např. internetové bankovnictví, interní systémy
- **Kontrolujte zařízení** – pravidelně sleduj, zda se neobjevují podezřelé aplikace nebo chování již instalovaných aplikací
- **Zamykání zařízení –** používej PIN, otisk prstu nebo rozpoznání obličeje.
- **Buď opatrný při půjčování zařízení** – nedávej telefon nebo notebook cizím osobám.
- **Sleduj účty na sociálních sítích** – zda nedochází k neautorizovanému přístupu.

Nesdílej polohu v reálném čase

Uživatelka z ČR na Instagramu sdílela fotku z dovolené s popiskem typu:

„Konečně na Mallorce! 🌴 #holiday #beachlife“.

- Fotka byla veřejná a obsahovala přesnou polohu díky GPS metadatům.
- Zloději, kteří sledovali její profil, zjistili, že není doma.
- Využili této informace a vloupali se do jejího bytu, zatímco byla na dovolené.
- Policie později potvrdila, že pachatelé sledovali sociální sítě a cíleně vybírali oběti, které zveřejňovaly svou nepřítomnost.

- Podobně sdílejí polohu také influenceři (z akce, hotelu, restaurace)
- Prozrazena poloha tajné základny díky sdílení polohy v aplikaci STRAVA.

Po návratu domů

- **Změňte hesla** – zejména pokud jsi se připojoval k veřejným sítím.
- **Zkontrolujte své online účty** – zda nedošlo k neobvyklé aktivitě (např. přihlášení z cizí IP adresy).
- **Proveďte rozsáhlejší antivirovou kontrolu** – na všech zařízeních, která jsi používal.
- **Odstraňte aplikace, které jste nainstalovali jen pro cestu** – např. místní dopravní aplikace.
- **Zhodnoťte své bezpečnostní chování** – co šlo dobře, co bys příště udělal jinak.

Další doporučení

Cestovní "čistá" zařízení

Pro cesty do rizikových oblastí použij separátní zařízení s minimem osobních dat. Po návratu ho můžeš kompletně obnovit do továrního nastavení.

Rozdělení účtů

Vytvoř si separátní e-mailové účty - jeden pro komunikaci s ubytováním a cestovními službami, druhý pro bankovnictví a citlivé služby.

Aktivuj "ztracený mód"

Nastav si vzdálené vyhledávání a mazání dat v systémových službách jako "Find My iPhone" nebo "Find My Device". V případě ztráty můžeš zařízení lokalizovat nebo vzdáleně vymazat.

Připojení na nezabezpečenou síť

- Bezpečný přenos dat na vnitřní síť a z ní je přes **VPN**. (**Virtual Private Network**)
- Pokud mohu, upřednostňuji datový přenos – využívám datový tarif.
- Není-li to možné nebo žádoucí, pak používám WiFi síť se známým provozovatelem a **zabezpečením WPA2**.
- K WiFi se připojuji jen na nezbytně nutnou dobu a po skončení přenosu dat síť okamžitě mažu ze zařízení.
- Požádám o zřízení VPN přístupu k vnitřní síti organizace, a to pouze tehdy, když jej potřebuji.
- Nepoužívám Free WiFi – tyto zóny mohou být odposlouchávány.
- Nenechávám své mobilní zařízení detekovat a připojovat se k neznámým sítím.

Tipy na bezpečnou domácí wifi síť

- Zaheslovat administrační rozhraní pro správu routeru.
- Aktualizovat firmware routeru.
- Nastavit zabezpečení WPA2 (šifrování komunikace).
- Nastavit vlastní název sítě (SSID) a případně ho skrýt.
- Nastavit síť pro hosty (guest režim) a vypnout WPS.
- Nastavit heslo (či hesla) pro jednotlivá SSID.
- Omezte možnost vzdálené správy vašeho routeru.
- Monitorujte, kdo je k síti připojen.

ODEMYKÁNÍ ZAŘÍZENÍ

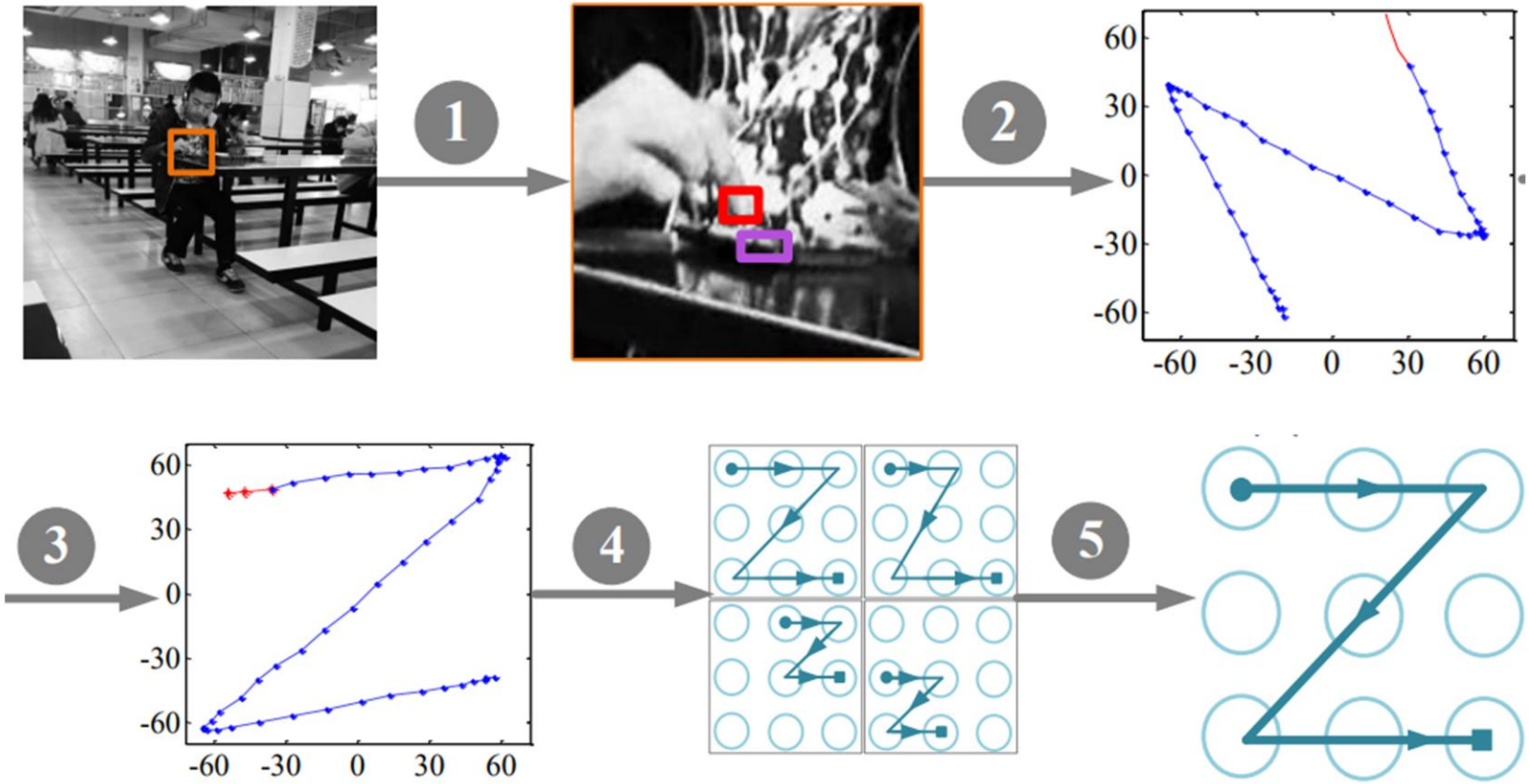
Tradiční metody odemykání mobilních zařízení

- **PIN kód:** Číselný kód, doporučovaný je 8 znaků. Je důležité, aby nebyl triviální.
- **Gesto:** Spojování bodů na obrazovce ve specifickém vzoru. Tato metoda je méně bezpečná, protože vzor může být snadno odpozorován.
- **Heslo:** Kombinace písmen, číslic a speciálních znaků.

Moderní metody odemykání mobilních zařízení

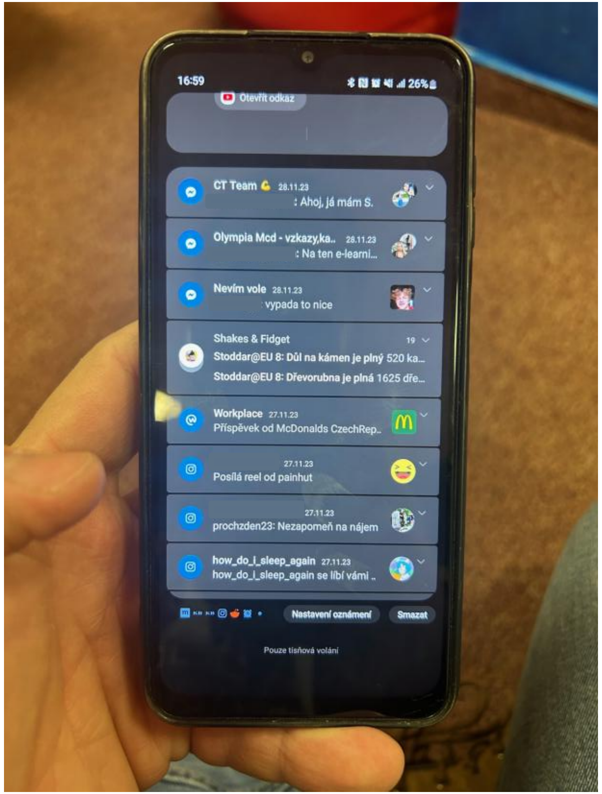
- **Otisk prstu:** Tato metoda využívá skener otisků prstů, který porovnává otisk prstu uživatele s uloženým vzorem.
- **Sken obličeje:** Tato metoda využívá kameru a pokročilé algoritmy k rozpoznání obličeje uživatele.
- **Sken duhovky:** Některá zařízení využívají skenování duhovky oka, což je velmi přesná metoda, protože duhovka má jedinečný vzor pro každého člověka.
- **Rozpoznání hlasu:** Tato metoda využívá analýzu hlasu uživatele k ověření uživatele. I když není tak běžná jako otisk prstu nebo sken obličeje.

Odpozorování gest



Když gesto není třeba znát

Národní úřad
pro kybernetickou
a informační bezpečnost



- **Uzamčený** – chráněný gestem
- Povolené plné notifikace na uzamčené obrazovce.
- Připojená NFC platební karta mBank spolu s výpisy o výběru z bankomatu.
- Zobrazené jméno majitele telefonu, zprávy, e-mailové notifikace, informace ze služby workplace a další podrobnosti.

Útočník by měl možnost získat z telefonu:

- kód ze SMS nebo aplikace (multifaktor po zadání jména a hesla ke službě/účtu),
- důvěrné informace pro krádež identity,
- informace pro dohledání majitele a jeho případné pronásledování.

- Díky notifikacím bylo možné dohledat majitele na sociální síti Facebook a telefon mu vrátit aniž by došlo k jeho zneužití.
- Nalezen v 7:15 minut ráno.
- Vrácen v 17:30 tentýž den.

Další vzdělávací aktivity

osveta.nukib.gov.cz

Průvodce portálem

Národní úřad
pro kybernetickou
a informační bezpečnost

Děkuji za pozornost