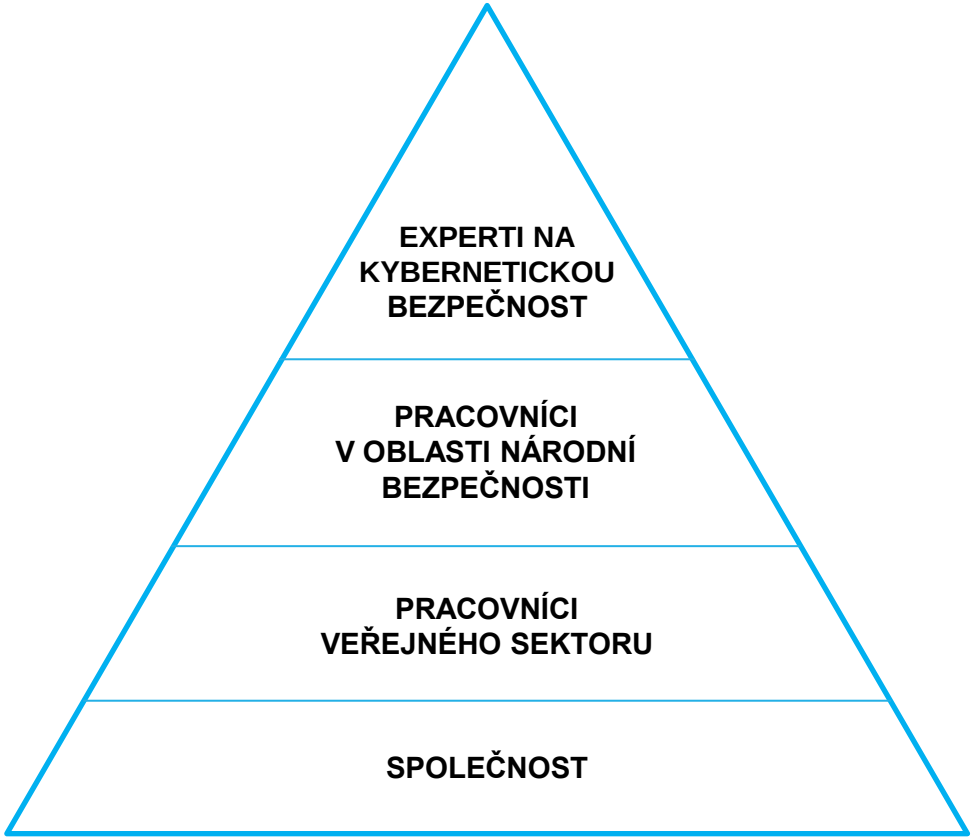
Digitální štít aneb základy kybernetické bezpečnosti

Martin Hájek

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.

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

Kdo za co odpovídá?

Zodpovědnost za přístup k počítači, tedy i k heslům, je na každém uživateli.

Stejně tak je na jednotlivcích i to, jestli dodržují zásady archivace, zálohování a další bezpečnostní předpisy.

V oblasti kybernetické kriminality 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“, „moje fotografie nejsou věc veřejná“ a další věci, které nás odmala učili.

Nastavení sítě a zásad bezpečnosti je věc jedna, ale jejich akceptování a každodenní dodržování je věc druhá.

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

Kybernetická bezpečnost

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

PRAVIDLA, OPATŘENÍ A PROSTŘEDKY

PRO OCHRANU UŽIVATELŮ A SYSTÉMU

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

Vlastnost přesnosti a úplnosti.

DOSTUPNOST – informace je dostupná

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.

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.

Jak mohou moje údaje utéct?

- **Odpozorováním údajů nebo hesla** – nezamčená kancelář, nezamčená obrazovka počítače, monitor viditelný z vnějších prostor (oknem na ulici, z vedlejší kanceláře, z chodby…), heslo na monitoru.
- **Špatně zvoleným heslem**, které lze snadno prolomit.
- **Nezajištěním** přenosných zařízení.
- **Připojením na nezabezpečenou síť** - veřejnou WiFi, nezabezpečené připojení v hotelu, MHD, a podobně.
- **Zadáním údajů na neznámý server** – phishing.
- **Zasláním údajů cizím, neověřeným osobám** třeba v rámci soukromé komunikace.

Jak na 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. Interval bývá nastaven vnitřním nařízeném.
- Heslo měníme vždy, když máme podezření na jeho únik.

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:

granát

Heslo musí obsahovat více než 8 znaků.

ruční granát

Heslo musí obsahovat alespoň jednu číslici.

2 ruční granáty

Heslo nesmí obsahovat diakritiku.

2 rucni granaty

Heslo nesmí obsahovat mezery.

2blbyrucnigranaty

Heslo musí obsahovat alespoň jedno velké písmeno.

2BLBYrucnigranaty

Heslo nesmí obsahovat více velkých písmen po sobě.

2BlbyRucniGranaty,UzMiKonecneDejteTenPristup

Heslo nesmí obsahovat interpunkci.

2BlbyRucniGranatyUzMiKonecneDejteTenBlbejPristup

Heslo musí obsahovat jeden speciální znak.

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

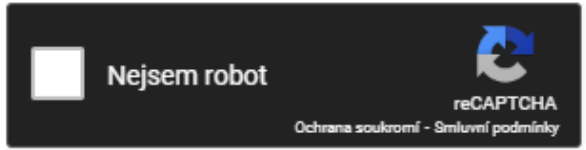
Generate →

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

Multifaktorové ověření

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,…)

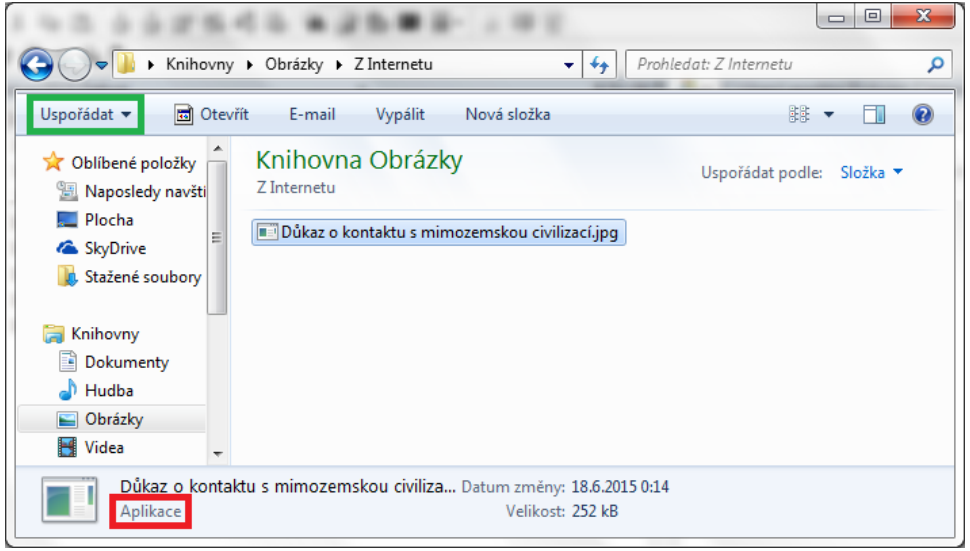
ŠKODLIVÉ SOUBORY

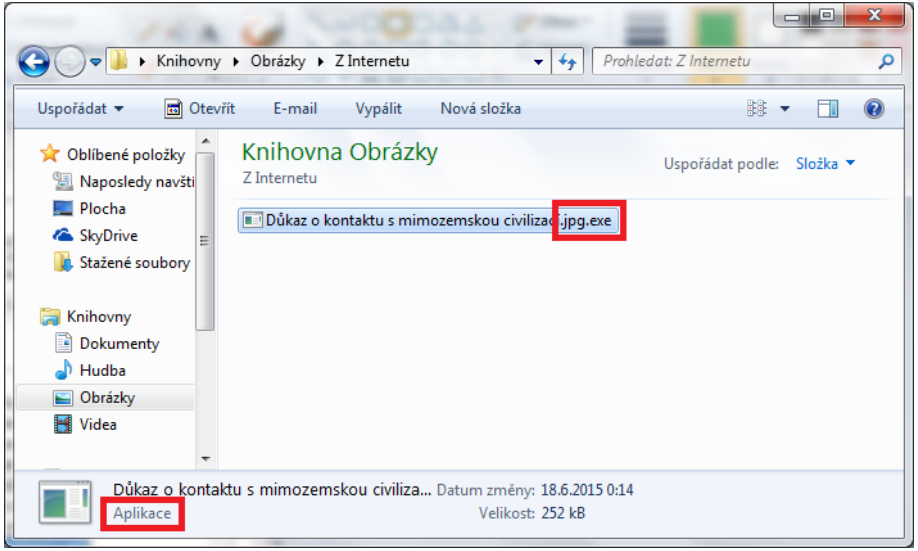
Co jsou škodlivé soubory?

- Soubory, které mohou ovlivnit fungování počítače, poškodit ho, nebo pomoci útočníkovi nad ním převzít kontrolu.
- Bývají to spustitelné soubory, které útočník velmi často maskuje za jiný soubor.
- Nejznámější příponou bývá *.exe
- Po otevření takového souboru může uživatel nainstalovat škodlivý program.
- Obvykle se tento druh soborů šíří prostřednictvím e-mailů, přenosných USB zařízení a dalších chytrých zařízení.
- V pracovním prostředí bývá obvykle spouštění podobných souborů zakázáno.

Maskování škodlivých souborů

- Útočníci velmi často spustitelné soubory maskují jako jiný druh.
- Využívají také archivu, do kterého mohou zabalit více souborů.
- Například přípony souborů se dají různě maskovat.





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/mobilní telefon
- 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.

Přenosná zařízení

- Nikdy nedávám do svého počítače žádné zařízení, které neprošlo antivirovou pračkou nebo důkladnou kontrolou. To platí i pro mobilní zařízení, telefony nebo fotoaparáty.
- Nalezená zařízení odevzdám na místo k tomu určené. Nepokouším se určit majitele tak, že se podívám na obsah.
- Papírové spisy mohou obsahovat velké množství údajů, pomocí kterých lze odvodit údaje přístupové.

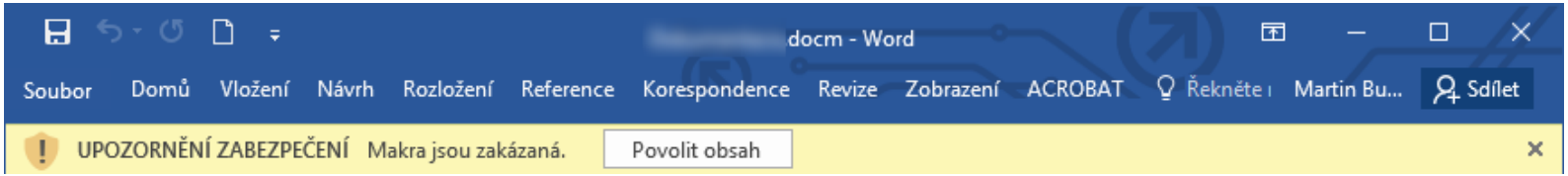
Svá zařízení nikomu nesvěřuji, pokud je dám do cizího počítače, prověřím je antivirovou pračkou nebo zkontroluji dle pokynů manažera bezpečnosti IT. Cizí zařízení nepřipojuji a nepoužívám. I dárky by měly být prověřeny, než je použiji. Škodlivý kód může nahrát už výrobce.

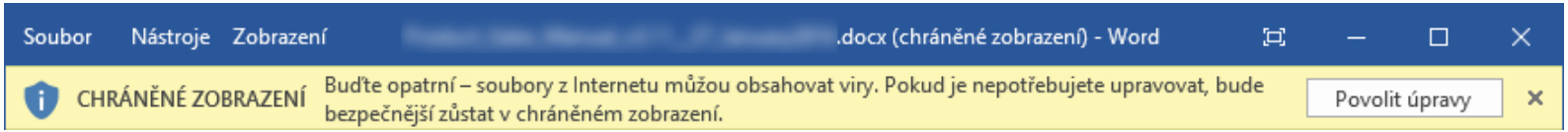
Makro

- Makra jsou pokročilé sady pravidel, které si můžeme vytvořit, aby za nás vykonávaly opakující se úkony.
- A opět také platí, že je útočníci umí zneužít. Mohou makru říct:

„Stáhni z tohoto odkazu tento škodlivý soubor, počkej v úkrytu na tohle, a pak vykonej tohle.“

- Z tohoto důvodu bývají makra v základním nastavení vypnutá a musejí se povolit.





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:

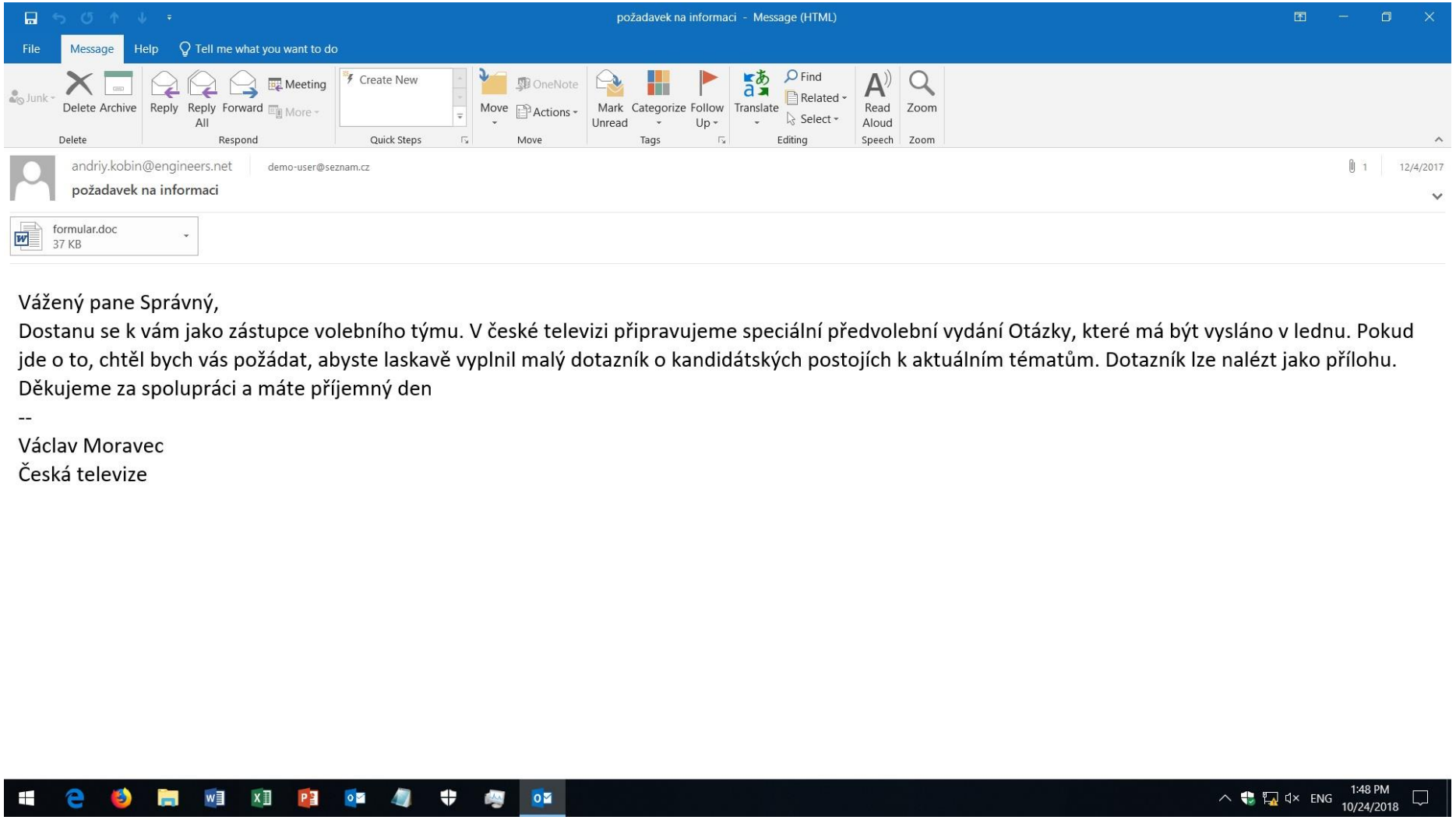
- přihlašovací údaje k různým webovým službám a aplikacím, hesla, čísla kreditních karet apod.

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

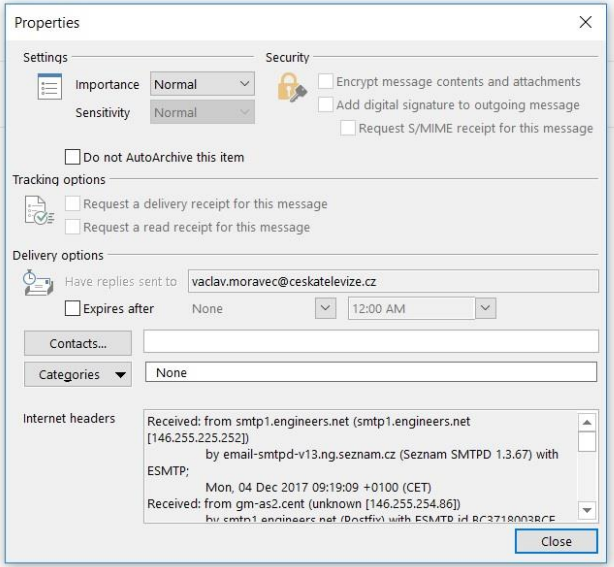
informace pro ČT

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



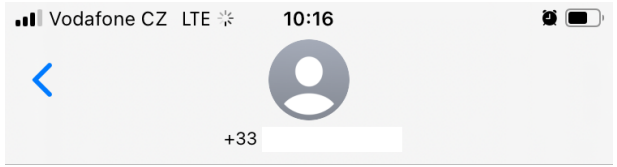
ENG 1:53 PM 10/24/2018

Doporučení pro e-mailovou komunikaci

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

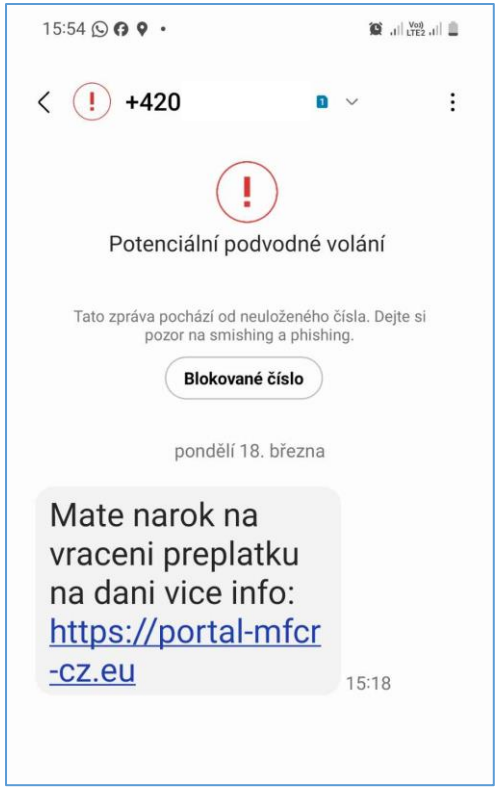
Nejčastější napadení počítače je právě přes e-mailovou schránku.

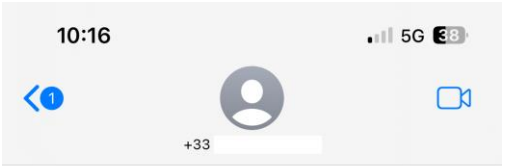
AKTUÁLNĚ – SMiShing



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

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

Ústav jaderného výzkumu

Kdy:

- Prosinec 2022

Co se stalo

- Ransomware zašifroval data na serverech
- Útok na ekonomický úsek ÚJV Řež → ekonomický systém měl výpadky → 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

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. V souvislosti s tím bychom měli dávat pozor i na QR kódy.
- Nenechávám své mobilní zařízení detekovat a připojovat se k neznámým sítím.

Tipy na bezpečnou domácí wifi síť

Národní úřad
pro kybernetickou
a informační bezpečnost

- 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.

Další vzdělávací aktivity

osveta.nukib.gov.cz

Průvodce portálem

Děkuji za pozornost