Kybernetická a informační bezpečnost

Markos Moras & Martin Hájek

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

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 infrastruktura

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.

- 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

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.

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

Činnost NÚKIB

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

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

Další aktivity

osveta.nukib.cz

Průvodce portálem

ZÁKLADNÍ BEZPEČNOSTNÍ POJMY A DOPORUČENÍ

Kybernetický prostor

Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací.

ODKAZ:
https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_2_vydani.pdf

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

Bezpečnostní hrozba a incident

HROZBA – něco, co může ohrozit uživatele nebo systém

Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.

INCIDENT – něco, co se už stalo a je třeba to řešit

Porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a komunikační technologie.

Bezpečnost internetu

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.

Kdo je to ten hacker?

HACKING

Cílená změna běžného fungování počítače/systému za pomocí skriptů a speciálních programů. Cílem bývá získávání informací a manipulace s daty.

HACKER

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

CRACKER

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

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 nebo spisů.
- **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.

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:

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.

Dvoufaktorové 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,…)

A kdo za to zodpovídá?

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.

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.

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

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.

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.

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

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.

Sociální inženýrství

NEOPATRNOST V KOMUNIKACI, DŮVĚŘIVOST, UNÁHLENOST,

Manipulativní jednání s cílem získat informace má mnoho podob.

Může být osobní: „Ale když mi jenom pošleš potvrzovací kód platby, nic se nemůže stát!“

Založené na soucitu: „Když mi to heslo nedáte a já vám počítač neopravím, šéf mě vyhodí!“

Založené na znalosti firemních pravidel: „Můj vedoucí, pan XY, chce, abych IHNED zkontroloval vzdálený přístup k vašemu počítači. Potřebuji vaše přístupové údaje.“

Tím, že věta obsahuje jméno skutečné osoby, získává na důvěryhodnosti. Přitom jméno vedoucího IT je často na webových stránkách firmy.

Sociální inženýrství – doporučení

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

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.

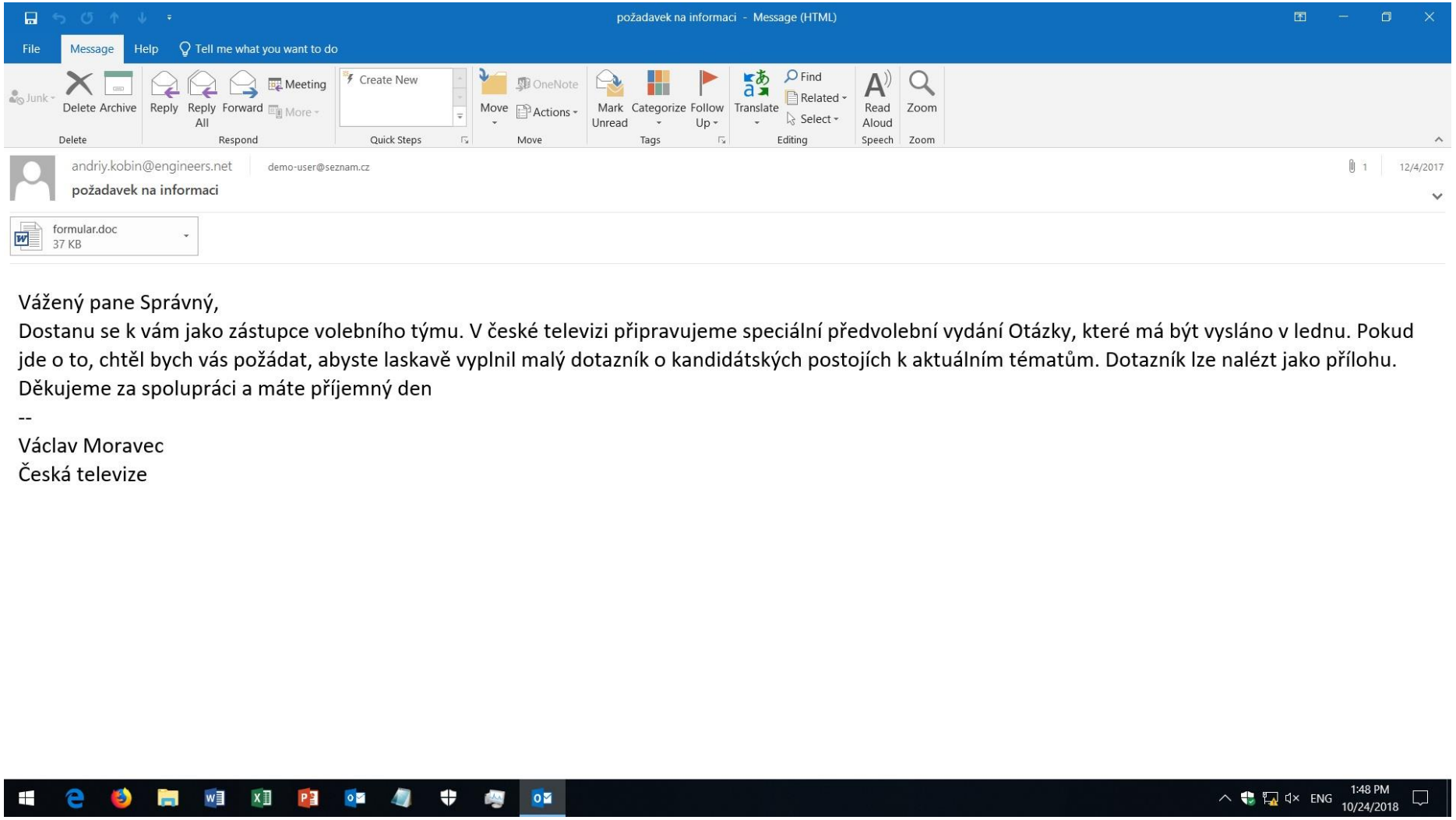
- Nejčastější napadení počítače je právě přes e-mailovou schránku.

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.


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

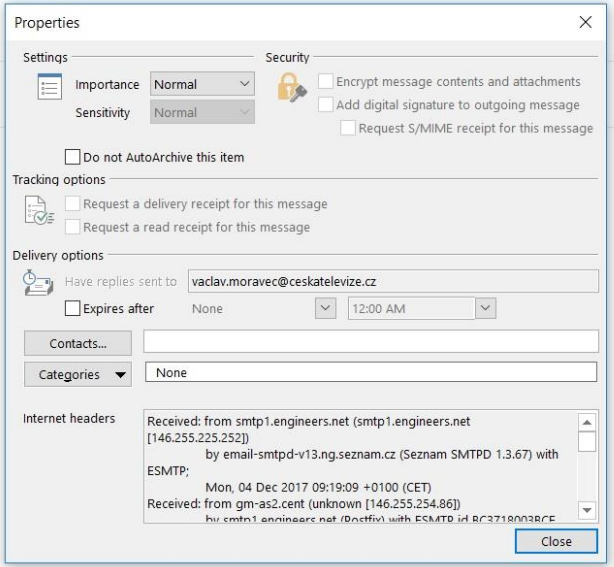
informace pro ČT

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

Obecné zásady bezpečnosti

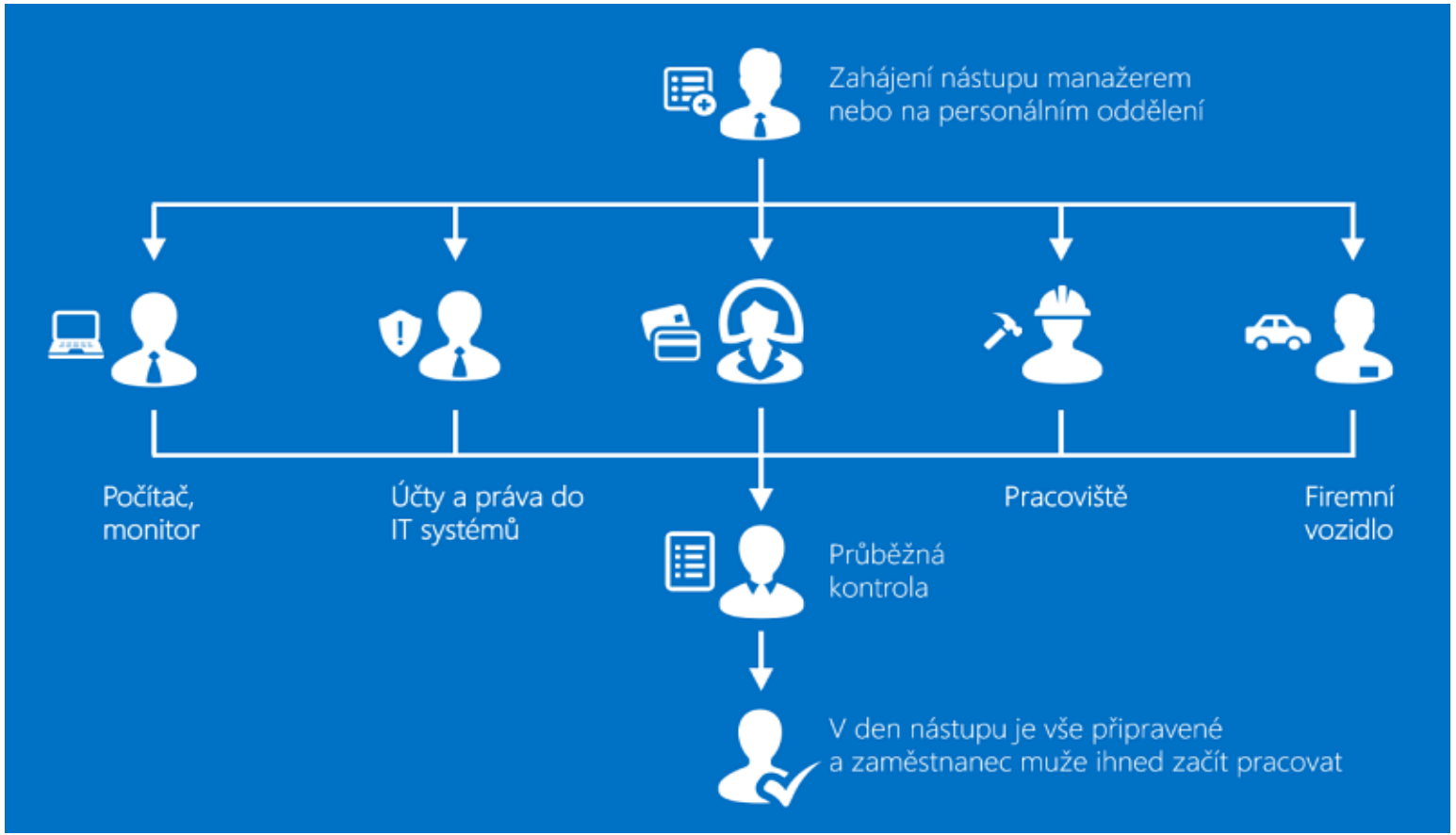
Bezpečnostní politika IT:
Pravidla, směrnice a praktiky, které rozhodují o tom, jak jsou aktiva včetně citlivých informací spravovány, chráněny a distribuovány uvnitř organizace a jejich systémů ICT.

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.

Ukázka kompetencí IT oddělení



Podle čeho je možné se řídit?

Certifikace organizace podle norem ISO/IEC zvyšuje úroveň bezpečnosti organizace.

Typy norem:

- ISO/IEC 27001 Management bezpečnosti informací (ISMS)
- ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Kodex postupů pro kontroly bezpečnosti informací.
- ČSN EN ISO 9000 Systémy managementu kvality.

ISO International Organization for Standardization

Zveřejnění údajů

Osobní údaje Alberta Rýhrše jsou dostupné na sociální síti Facebook… **citlivým údajem** je třeba to, že Albert byl původně žena, což dokazuje tvar jeho pánve, který nese klasické ženské znaky.

Registrace nového uživatele

Kontaktní údaje

Jméno:
Příjmení:
Telefon:

Vytvoření účtu

E-mail:
Přihlašovací jméno:
Heslo:
Heslo znovu:

Fakturační údaje

Ulice a číslo popisné:
Obec:
PSČ:
Stát:

☑ souhlasím se zasíláním informačních materiálů a obchodních nabídek od společnosti XYZ s.r.o. na výše uvedený e-mail

Zaregistrovat

Podobně i vaše údaje mohou být dostupné, pokud se registrujete na neznámém serveru.

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 včetně záloh
- 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

ŠKODLIVÝ KÓD

Malware – proč je (zne)užíván

- Infikovat počítače s cílem těžit kryptoměnu (Bitcoin)
- Přinutit oběť vydat osobní údaje (krádeže identity)
- Získat informace z platebních karet nebo jiných finančních dat (obohacení)
- Převzít kontrolu nad velkým množstvím počítačů, z kterých se bude následně útočit (DoS útok – Denial of Service)

TYPY MALWARU

POČÍTAČOVÉ VIRY

Malware, který se šíří z počítače na počítač tím, že se připojí k jiným aplikacím.

Následně může působit nežádoucí a nebezpečnou činnost. Má v sobě obvykle zabudován mechanismus dalšího šíření či mutací

SCAREWARE

Malware, který při procházení webu zobrazí výstražné zprávy s varováním, že váš počítač je infikován nebo že se v něm vyskytl virus.

Využívají se k tomuto účelu vyskakovací okna nebo nové záložky.

ADWARE

Programy, které znepříjemňují práci reklamní aplikací. Tyto prezentace mohou mít různou úroveň agresivity - od běžných bannerů až po neustále vyskakující pop-up okna nebo ikony v oznamovací oblasti

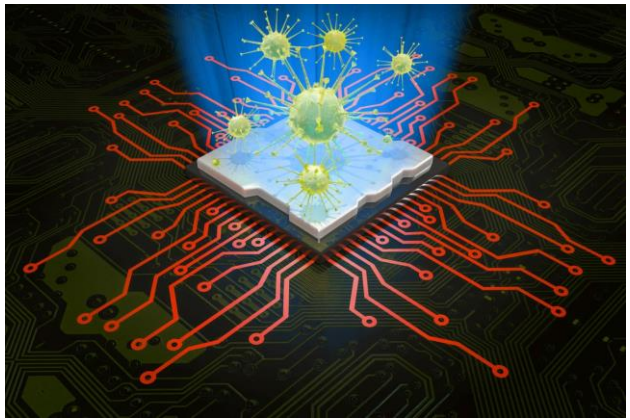
SPYWARE

Program, který využívá internetové stránky k odesílání dat z počítače nebo mobilního telefonu či jiného zařízení bez vědomí jeho uživatele.

Říká se mu špionážní software.

ČERVI

Samostatná množina softwaru, který je schopný vytvářet své kopie, které rozesílá do dalších systémů (sítí), kde vyvíjí svoji nelegální činnost. Často slouží ke hledání bezpečnostních skulin v systémech nebo v poštovních programech.



TROJSKÉ KONĚ

Program, který plní na první pohled nějakou užitečnou funkci, ale ve skutečnosti má ještě nějakou skrytou škodlivou funkci. Trojský kůň se sám nereplikuje, šíří se díky viditelně užitné funkci, kterou poskytuje.

Bezsouborový malware

- Tento typ škodlivého softwaru využívá legitimní programy k infikování počítače.
- Při útocích bezsouborového malwaru na registry nejsou zanechány žádné
- soubory ke skenování a žádné škodlivé procesy ke zjištění.
- Není závislý na souborech a nezanechává žádnou stopu, takže je náročné jej
- zjistit a odstranit.

Obrana proti malwaru 1/2

- Důkladná segmentace sítě.
- Zabezpečit privilegované účty.
- Využívat pouze podporované operační systémy.
- Monitorovat zranitelnosti na perimetru sítě
- Monitorování síťového provozu.
- Provádět pravidelné audity kybernetické bezpečnosti
- Offline zálohy

Obrana proti malwaru 2/2

- Mít vytištěné krizové plány a testovat je
- Mít kvalitní antivirové zabezpečení
- Školit běžné zaměstnance i odborníky.
- Osvěta proti phishingu, sociálnímu inženýrství
- Nestahovat programy a aplikace z neznámých zdrojů
- Neotevírat přílohy nevyžádaných emailů nebo ze zpráv od neznámých kontaktů na sociálních sítích
- Neotvírat webové stránky s pochybným obsahem

Jak zjistím nákazu v počítači?

- Počítač má nízký výkon, nepracuje správně.
- Neplánované přesměrování na neznámou stránku nebo zobrazení webů, které
- jsme nechtěli navštívit
- Upozornění na infekci s nabídkou řešení k jejímu odstranění
- Problémy s vypínáním, spuštěním nebo restartem počítače
- Reklamy, které se svévolně otevírají při prohlížení

Děkuji za pozornost