MUNI
ICS

Kyberbezpečnost

Tomáš Plesník et al.

CSIRT-MU, 1. 12. 2021

Co nás dnes čeká?

Kyberhygiena

- 1. přednáška – 24. 11. 2021
- *„Těžko na cvičišti…“*
- Jak se bránit

Kybernetické útoky

- 2. přednáška – 1. 12. 2021
- *„Lehko na bojišti!“*
- **Čemu se bránit**

Kyberhygiena – opakování

- Hesla
- Zabezpečení zařízení
- (Ne)bezpečí na síti
- Bezpečnost e-mailové komunikace
- Digitální identity

Kyberhygiena – opakování

- **Hesla – základní mechanismus autentizace**
  - **Frázová hesla** – zapamatovatelná a jedinečná hesla (délka >= 3 slova, verše, říkanky)
  - **Prolomení hesel** – (sociální inženýrství, útoky hrubou silou, samotní uživatelé)
  - **Správce hesel** – bezpečný trezor chráněný „hlavním“ heslem (možnost generování hesel)
  - **Vícefaktorová autentizace** – pokročilejší vrstva ochrany proti prolomení, typicky 2FA
  - **Biometrie** – budoucnost vícefaktorové autentizace, problém zneužití, problém revokace
  - **Překonané metody** – hesla na papírcích, rotace + pamatování si hesel, speciální znaky

Kyberhygiena – opakování

- **Zabezpečení zařízení – vstupní branou do světa internetu**
  - **Uzamykání obrazovky** – snižuje riziko zneužití dat či (PIN, heslo, gesto, biometrika)
  - **Náhledy notifikací** – odhalují naše soukromí, kompromis nastavit pouze jména osob
  - **Antivirové řešení** – síto filtrující nebezpečí digitálního světa (SW, malware, síťový provoz)
  - **Pravidelné aktualizace** – poskytují vyšší bezpečnost SW i HW (oprava chyb, vylepšení)
  - **Testované zálohy** – ochrana před ztrátou, poškozením či zašifrováním dat (on-line řešení)
  - **Co dělat při ztrátě** – využití on-line služeb typu „Najdi moje zařízení“

Kyberhygiena – opakování

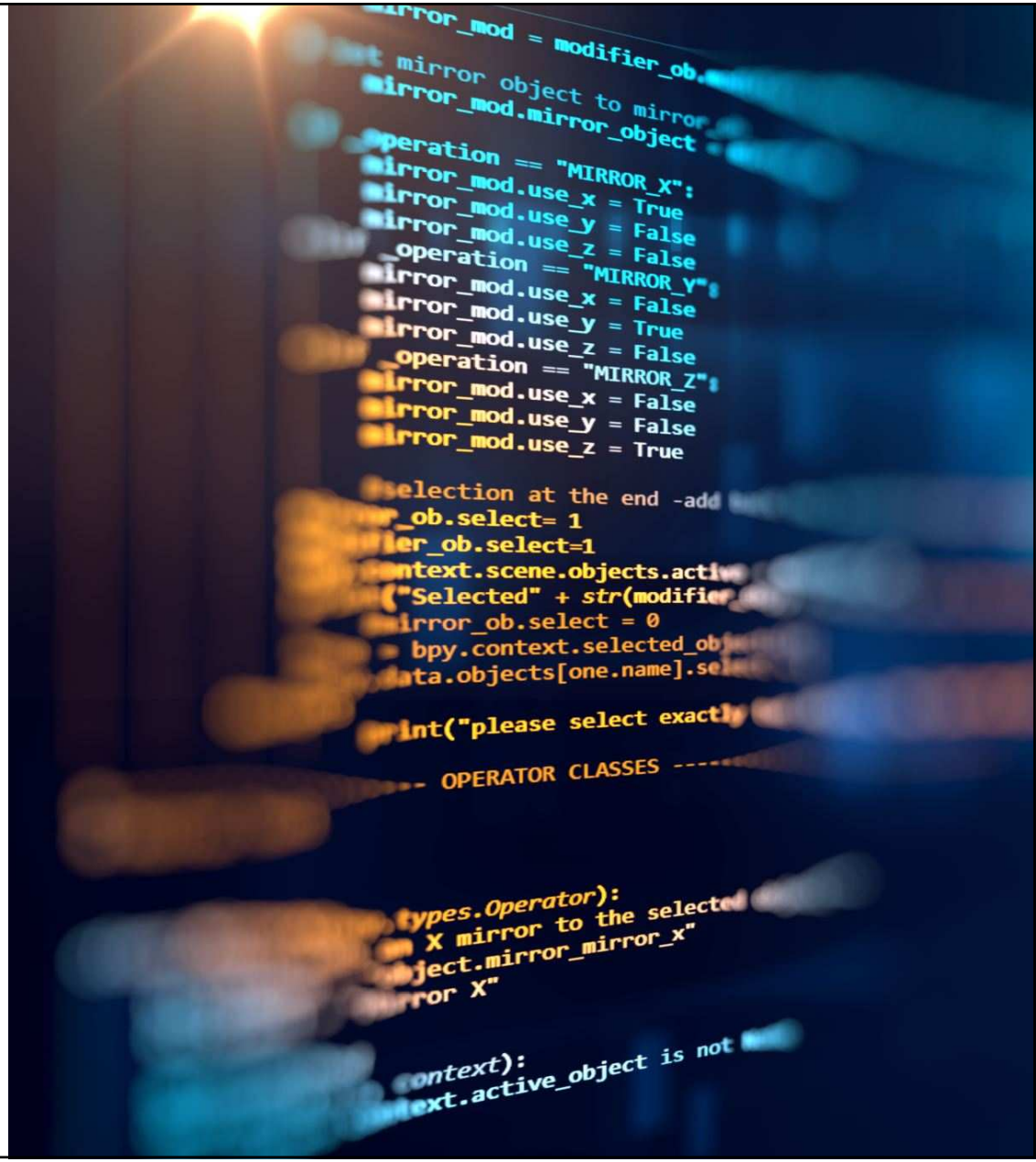
- **(Ne)bezpečí na síti – jak se bezpečně připojit na internet**
  - **Veřejná WiFi (bez hesla)** – velké bezpečnostní riziko pro citlivé údaje a data
  - **Veřejná WiFi (s heslem)** – o něco bezpečnější, ale stále Vás připojení uživatelé
  - **Virtuální privátní síť** – pomyslný tunel do „bezpečné“ sítě, do kterého útočník nevidí
  - **Eduroam** – infrastruktura provozovaná mezinárodní výzkumnou a vzdělávací komunitou

Kyberhygiena – opakování

- **Bezpečnost e-mailové komunikace – nutnost kritického myšlení**
  - **E-mailová zpráva** – tvořena hlavičkou a tělem
  - **Elektronický podpis** – zajišťuje integritu a nepopiratelnost přenášené zprávy a odesilatele
  - **Šifrování** – zajišťuje důvěrnost přenášené zprávy
- **Digitální identita – reflektuje nás a naše chování v online světě**
  - **Digitální identita** – tvořena naší digitální stopou (historie prohlížení, cookies, nákupy)
  - **Elektronická identita** – přihlašování se do IS státu (e-občanka, mojeID, BankID)

MUNI
ICS

Kybernetické útoky



Definice

Kybernetický útok

„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“

Zdroj: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

Kybernetické útoky

Nejčastější typy:

- Techniky sociálního inženýrství
- Sextortion
- Malware
- Ransomware

Méně časté:

- Odepření služby (DDoS)
- Man-in-the-Middle
- Drive-by-download

Kybernetické útoky – NÚKIB (říjen 2021)

Trendy v kybernetické bezpečnosti za říjen pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Podobně jako v předchozím měsíci NÚKIB v říjnu řešil phishingové kampaně. Dva povinné subjekty dle zákona o kybernetické bezpečnosti v říjnu odhalily kompromitované e-mailové účty svých uživatelů, kteří po prokliku z phishingové zprávy zadali přihlašovací údaje do falešného formuláře. Útočníci z jejich účtů dále rozesílali phishingové e-maily a snažili se tak proniknout do dalších organizací.

Malware

V říjnových incidentech se objevily tři škodlivé kódy - Dridex, RemCom a jeden coinminer.
První z nich, Dridex, NÚKIB objevil v rámci vlastního šetření na serverech jedné české společnosti, kde malware hostoval svou C2 infrastrukturu. Dridex může mít několik funkcionalit. Může detekovat bankovní aplikace, získávat k nim přihlašovací údaje, stahovat další škodlivé kódy nebo zaznamenávat úhozy na klávesnici. Kyberbezpečností společnosti Dridex připisují skupině známé jako Evil Corp, která cílí na organizace napříč sektory. V posledních dvou měsících aktivita spojená s malwarem Dridex roste.

Zranitelnosti

NÚKIB se v říjnu aktivně zabýval novou zranitelností CVE-2021-41773, která cílí na Apache HTTP Server. Ten je jedním z globálně nejvíce používaných webových serverů v prostředích Windows i Unix. Zneužití zranitelnosti umožňuje útočníkovi instalovat malware, kontrolovat systém a stahovat přihlašovací údaje.

NÚKIB o této zranitelnosti sice neinformoval veřejně na svých stránkách, ale upozornil povinné subjekty, jejichž servery byly zranitelné, a poslal jim doporučení pro řešení situace.

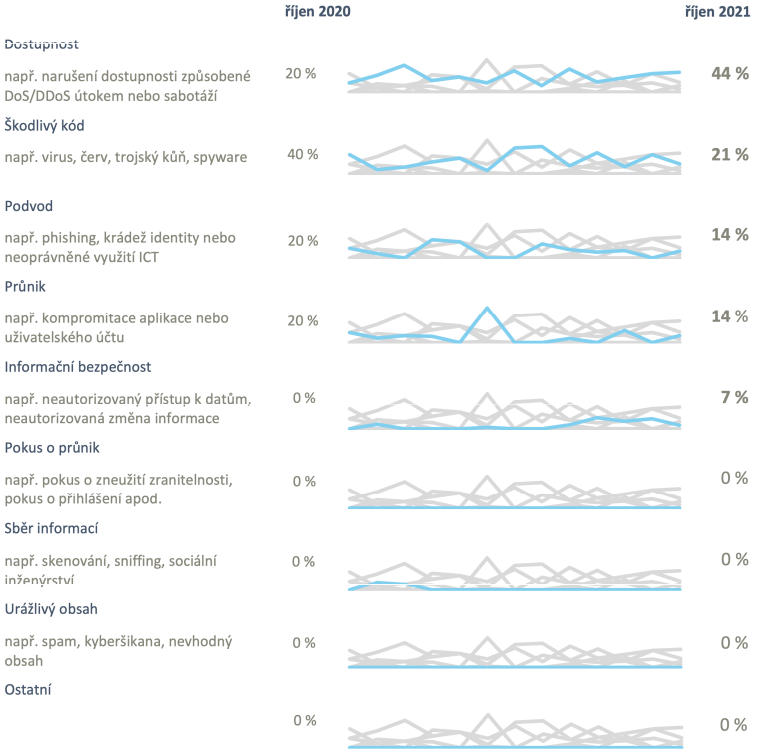
Ransomware

NÚKIB v říjnu řešil jeden případ ransomwaru. Jednalo se o ransomware LockBit, který zašifroval část infrastruktury soukromé společnosti a na svých stránkách vyhrožoval zveřejněním jejích dat.

LockBit je ransomware poskytovaný jako služba (RaaS). Podle dat RansomWatch se jedná o velmi rozšířený kód. V roce 2021 je zatím druhým nejrozšířenějším ransomwarem, který napadá organizace po celém světě.

Útoky na dostupnost

Oproti minulému měsíci, kdy ve statistikách NÚKIB nebyl žádný DoS nebo DDoS útok, se v říjnu objevily tři. Žádný z nich ale neměl vážné dopady. Všechny ovlivnily dostupnost služeb maximálně do 15 min a napadené organizace se s nimi vypořádaly pomocí vlastních prostředků.



Zdroj: https://www.nukib.cz/download/publikace/vyzkum/Kyberneticke_incidenty_2021-10.pdf

MUNI ICS

Motivace útočníků

- **Finanční zisk** – jasná motivace za účelem obohacení
- **Výzva a soupeření** – nejen jedinci, ale také státní aktéři
- **Pomsta** – neutralizace či poškození „nepřítele“
- **Vydíraní** – psychologický, politický či ekonomický záměr
- **Škodolibost** – konkurenční boj
- **Pokusy „script kiddies“** – první dětské krůčky
- **Hacktivismus** – spojením hackingu a aktivismu, politiky a technologie

Jsou KB útoky bežné?

- **Po celém světě neustále probíhá velké množství útoků**
  - V roce 2019 KB útok každých **39 sekund**, v roce 2021 již každých **11 sekund** (ransomware)
- **Převládají generické útoky na uživatele (IT již dostatečně odolné)**
  - Masivní, jednoduché, cenově efektivní a hlavně úspěšné
  - Techniky sociálního inženýrství, sextortion, malware + ransomware, DDoS
- **Můžete se přesvědčit na vlastní oči**
  - https://cybermap.kaspersky.com/

Situace (nejen) na MUNI

- **Zvyšující se počet KB událostí a incidentů** (zdroj: CSIRT-MU)
  - 2019: 111 317 pokusů o KB útok a 541 incidentů (ručně řešených)
  - 2020: 121 290 pokusů (nárůst o **9 %**) o KB útok a **1 494** incidentů (nárůst o **200 %**)
- **Varování NÚKIB ze dne 24. 2. 2021**
  - Č.j. 1506/2021-NÚKIB-E/310
  - **55–70 % pravděpodobnost** útoků typu ransomware v **horizontu 1-2 let** na VVŠ v ČR
  - Ohrožen výzkum a vývoj (obecně pak Know-how) na VVŠ
- **Útoky na nemocnice na jaře 2020 a knihovny na jaře 2021**

MUNI jako zdroj/cíl KB útoků

- **Druhá největší** univerzita v ČR
- Celkem **10** fakult
- **6 300+** zaměstnanců a **33 000+** studentů
- **27 000+** denně komunikujících IP adres
- **2** spravované VIS (IS MU a ESIS MU)
- **2x 40GE** připojení do akademické sítě Cesnet2
- **1x** Kyberbezpečnostní tým CSIRT-MU

MUNI ICS

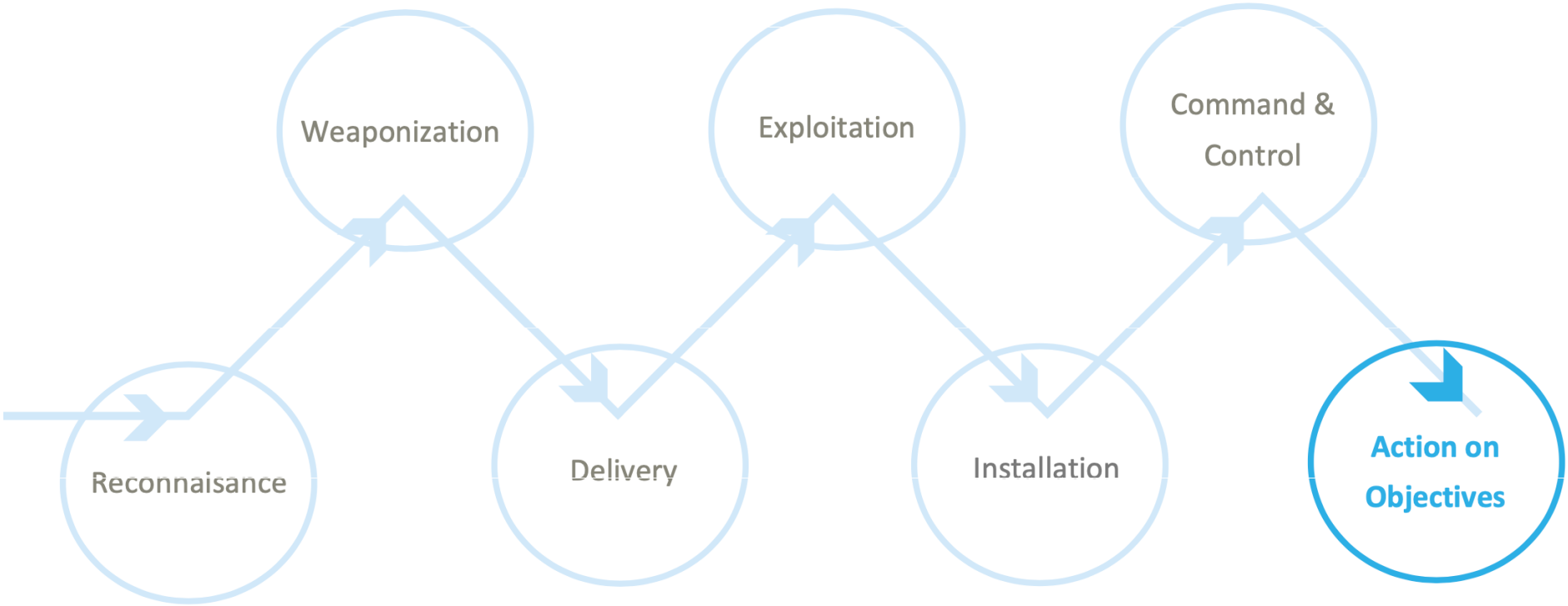
Útoky na MUNI

- **Útoky na uživatele**
  - Phishingové a spear-phishingové kampaně
  - Sextortion kampaně
  - Malware kampaně (typicky spojené ransomware)
  - Vishing
- **Útoky na IT**
  - Zneužití zranitelností
  - DDoS útoky
  - Kompromitace strojů – zastaralé, nezabezpečené či nespravované SW a HW

Jak to (zjednodušene) funguje v praxi?

- **Fáze 1**: průzkum prostředí
- **Fáze 2**: skenování cíle
- **Fáze 3**: získání přístupu
- **Fáze 4**: využití/udržování přístupu

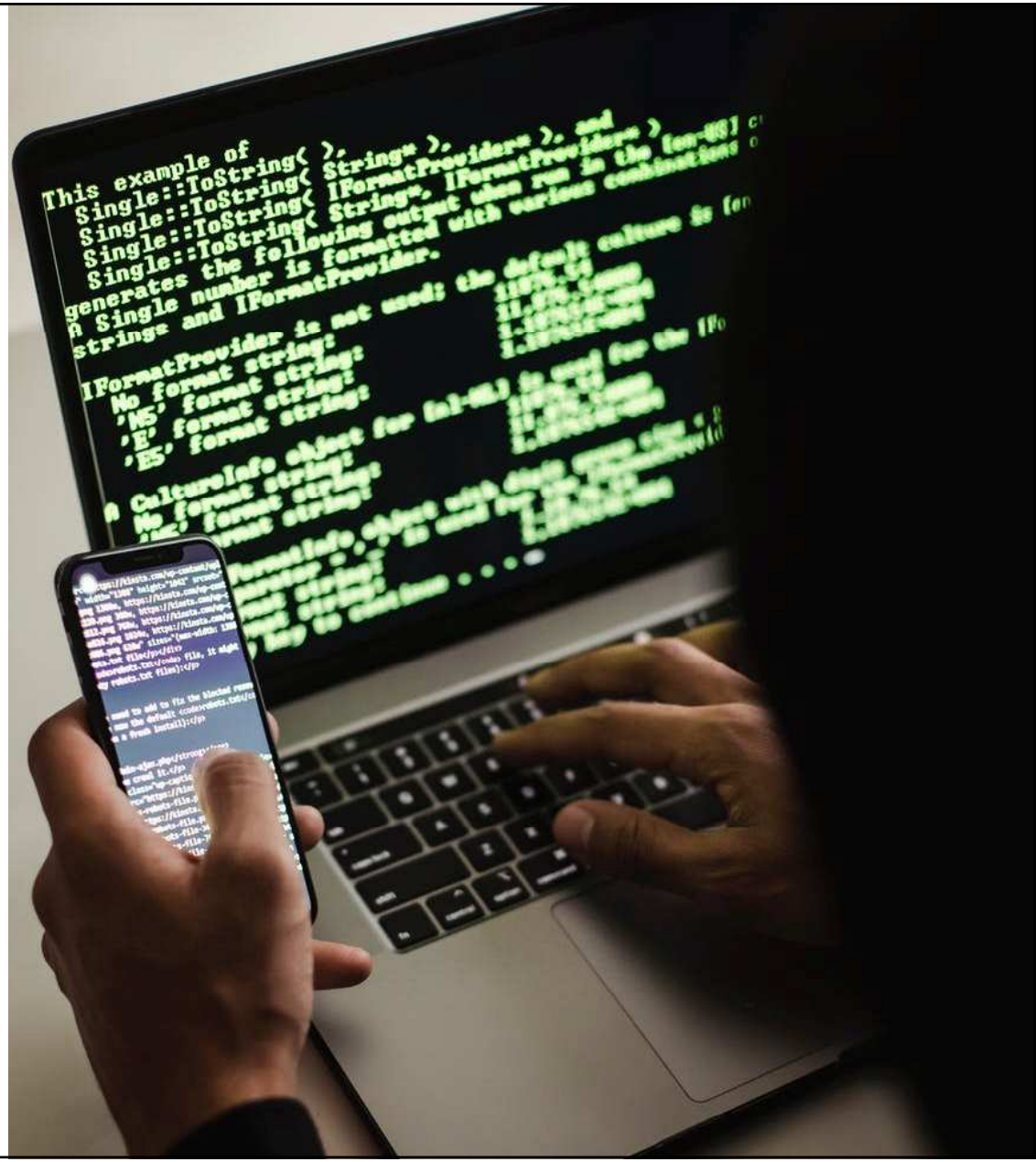
Jak to (častěji) funguje v praxi?



MUNI
ICS

MUNI
ICS

Najčastejší formy kybernetických útoků



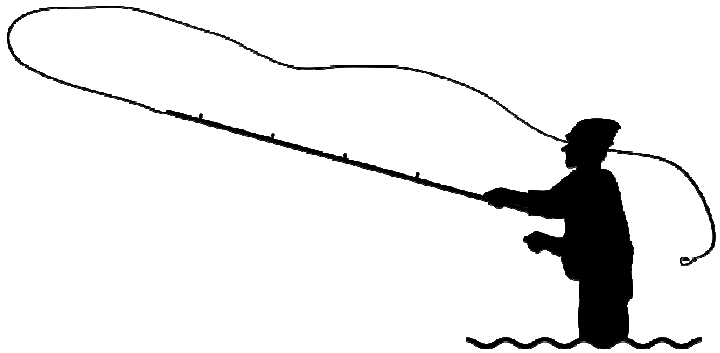
MUNI
ICS

Techniky sociálního inženýrství

Techniky sociálního inženýrství

- Využívají **psychologickou manipulaci**, zneužívají naši zvědavost, strach či nepozornost **k vylákaní přihlašovacích nebo osobních údajů**.

- **Phishing**
- **Spear-phishing**
- Vishing
- Baiting
- Trashing



MUNI
ICS

Kurz technik sociálního inženýrství

Příběhy sociálního inženýrství

KAPITOLY

Zdroj: https://security.muni.cz/socialni_inzenyrstvi

MUNI
ICS

Phishing

Phishing

- Jedna z **nejčastějších technik** sociálního inženýrství
- Za účelem **vylákání přihlašovacích údajů**
- Často **generické varianty** – anglické mutace
- **Špatná čeština** – použití překladače
- Užívané varianty:
  - Generic phishing – požadavek na přihlašovací údaje přímo součást textu zprávy
  - URL phishing – odkaz na URL v těle e-mailu
  - Malware phishing – zaslání malware v příloze e-mailu

Phishing – příklad

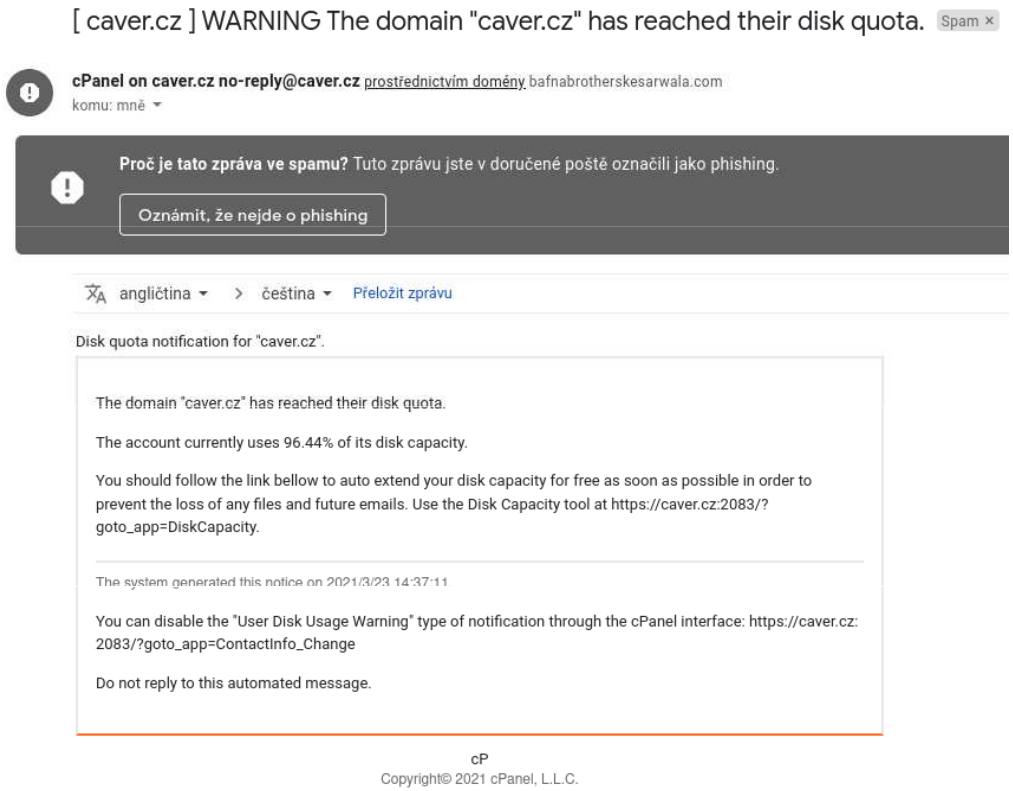
ZAČNĚTE SI UŽÍVAT NOVOU PLATFORMU PHIL.MUNI.CZ, ABYSTE SE VYHNULI ZTRÁTĚ SVÉHO ÚČTU PRO WEBMAIL. KLIKNĚTE ZDE [1] PRO OVĚŘENÍ VAŠÍ NOVÉ PLATFORMY PHIL.MUNI.CZ PODLE POKYNŮ ADMIN HELP DESK, POKUD NEBUDE DO 24 HODIN OVĚŘENA, BUDOU VŠECHNY ZPRÁVY DORUČENÉ POŠTY SMAZÁNY A VÁŠ WEBOVÝ ÚČET BUDE UKONČEN.

PODPORA
VEDENÍ TÝMU
PHIL.MUNI.CZ © COPYRIGHT

Links:
---
[1] http://mailphilmunizsquirrelmailsrcloginph9.mw.lt/

MUNI ICS

Phishing – příklad



[caver.cz] WARNING The domain "caver.cz" has reached their disk quota. Spam ×

cPanel on caver.cz no-reply@caver.cz prostřednictvím domény bafnabrotherskesarwala.com
komu: mně

Proč je tato zpráva ve spamu? Tuto zprávu jste v doručené poště označili jako phishing.

Oznámit, že nejde o phishing

angličtina > čeština Přeložit zprávu

Disk quota notification for "caver.cz".

The domain "caver.cz" has reached their disk quota.

The account currently uses 96.44% of its disk capacity.

You should follow the link bellow to auto extend your disk capacity for free as soon as possible in order to prevent the loss of any files and future emails. Use the Disk Capacity tool at https://caver.cz:2083/?goto_app=DiskCapacity.

The system generated this notice on 2021/3/23 14:37:11

You can disable the "User Disk Usage Warning" type of notification through the cPanel interface: https://caver.cz:2083/?goto_app=ContactInfo_Change

Do not reply to this automated message.

cP
Copyright© 2021 cPanel, L.L.C.

MUNI ICS

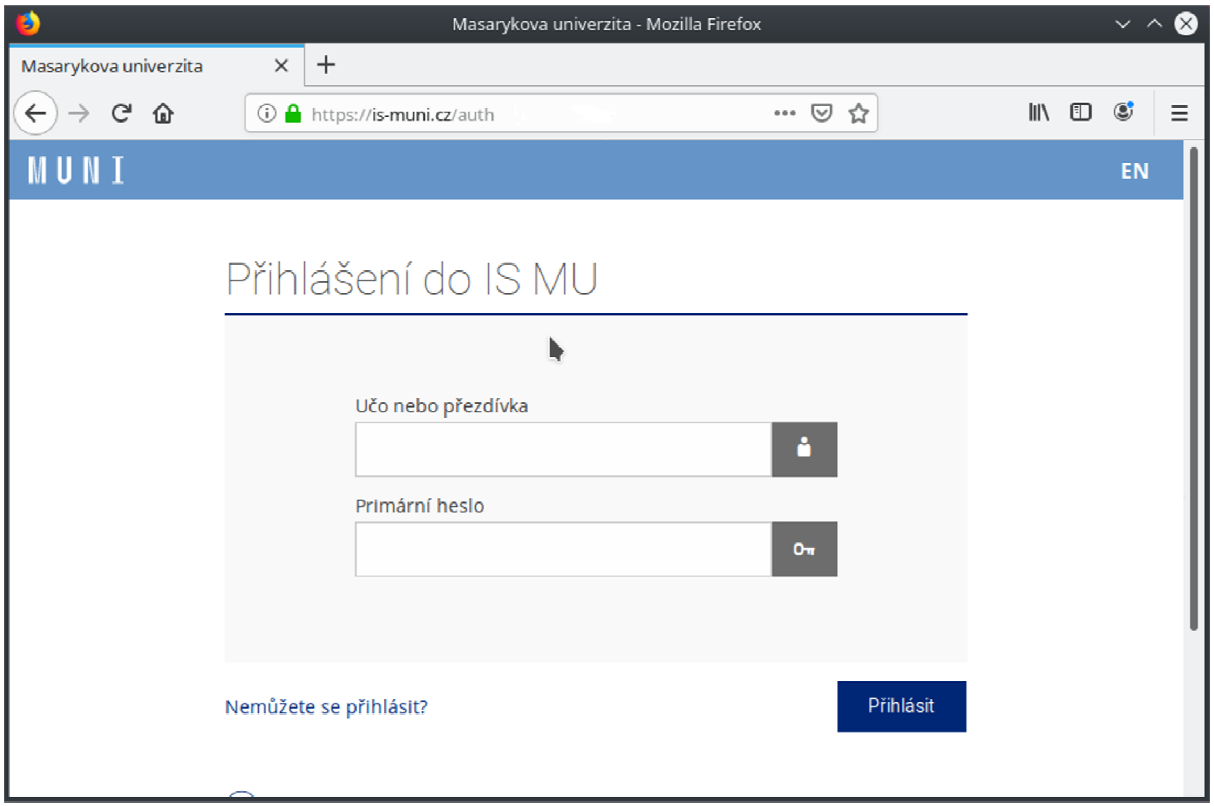
MUNI
ICS

Spear-phishing

Spear-phishing

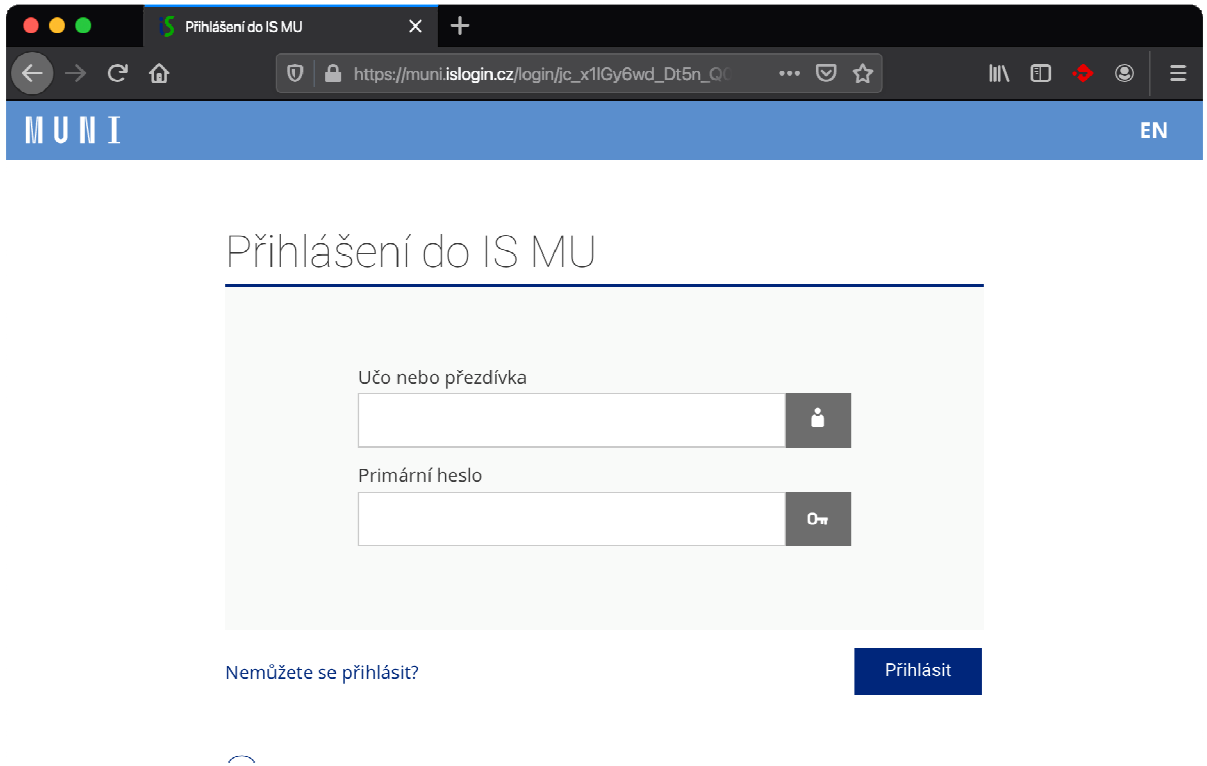
- **Pokročilejší verze phishingu**, které je již přímo zacílena
- **Důkladné zpracování**, včetně jazykové stránky
- Přesně zamířena na **správné osoby či místa v organizaci**
- **Těžko rozpoznatelné** i pro zkušené uživatele (pouze malé a detailní rozdíly)
- Většinou předchází **delší a hlubší sledování cíle** (oběti)
- Typicky **prvotní fází** většího a sofistikovaného útoku
  - Hrozba **Emotet-Trickbot-Ryuk** (Downloader-Malware-Ransomware)

Jedná se o legitimní přihlášení do IS MU?



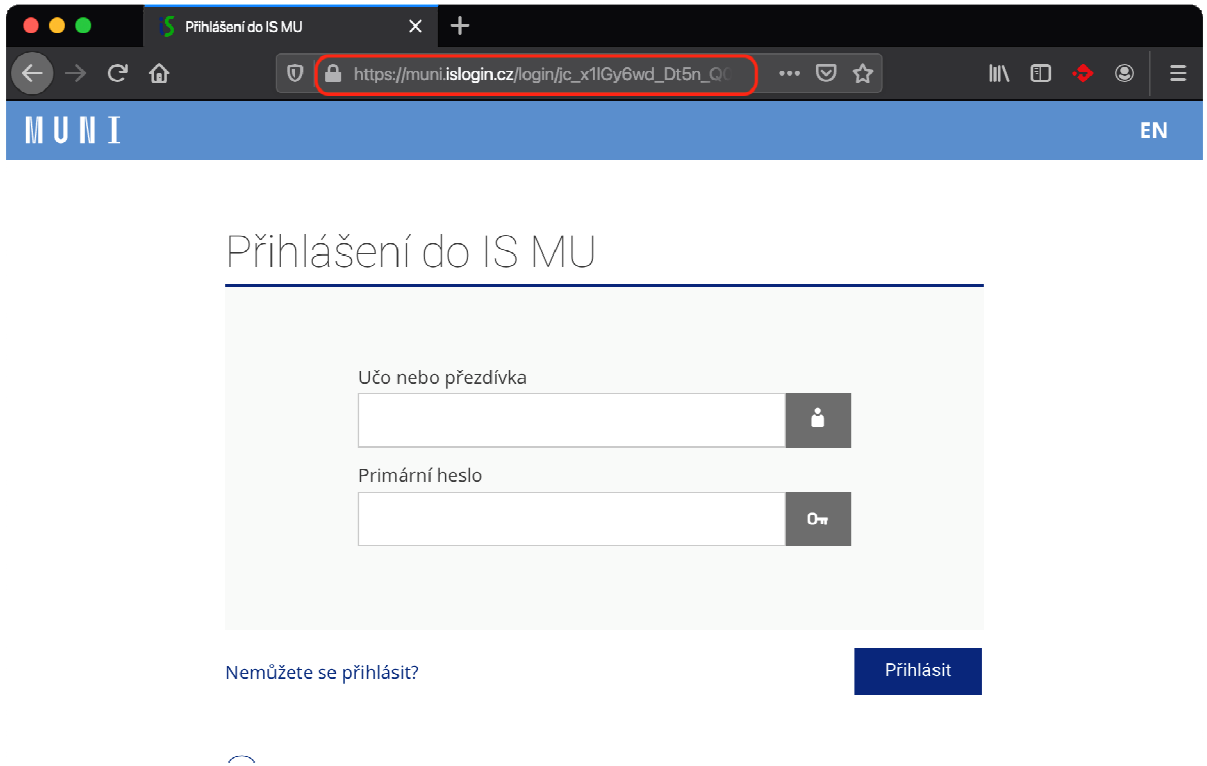
MUNI ICS

A co toto?



MUNI ICS

Kde je rozdíl?



MUNI ICS

Spear-phishing – příklad

Od: Masarykova univerzita Informační systém <alois.krobot@upol.cz>
Předmět: 27. pondělí říjen 2020
Datum: 27. října 2020 10:16:23 SEČ
Komu: [redacted]

MUNI Masarykova univerzita

2 Nové oznámení týkající se vašich mezd 2020

https://is.muni.cz/cz/Výplatní páska/2020/form.pdf

(c) 2020 Masaryk Univerzita

webmaster-up@muni.cz

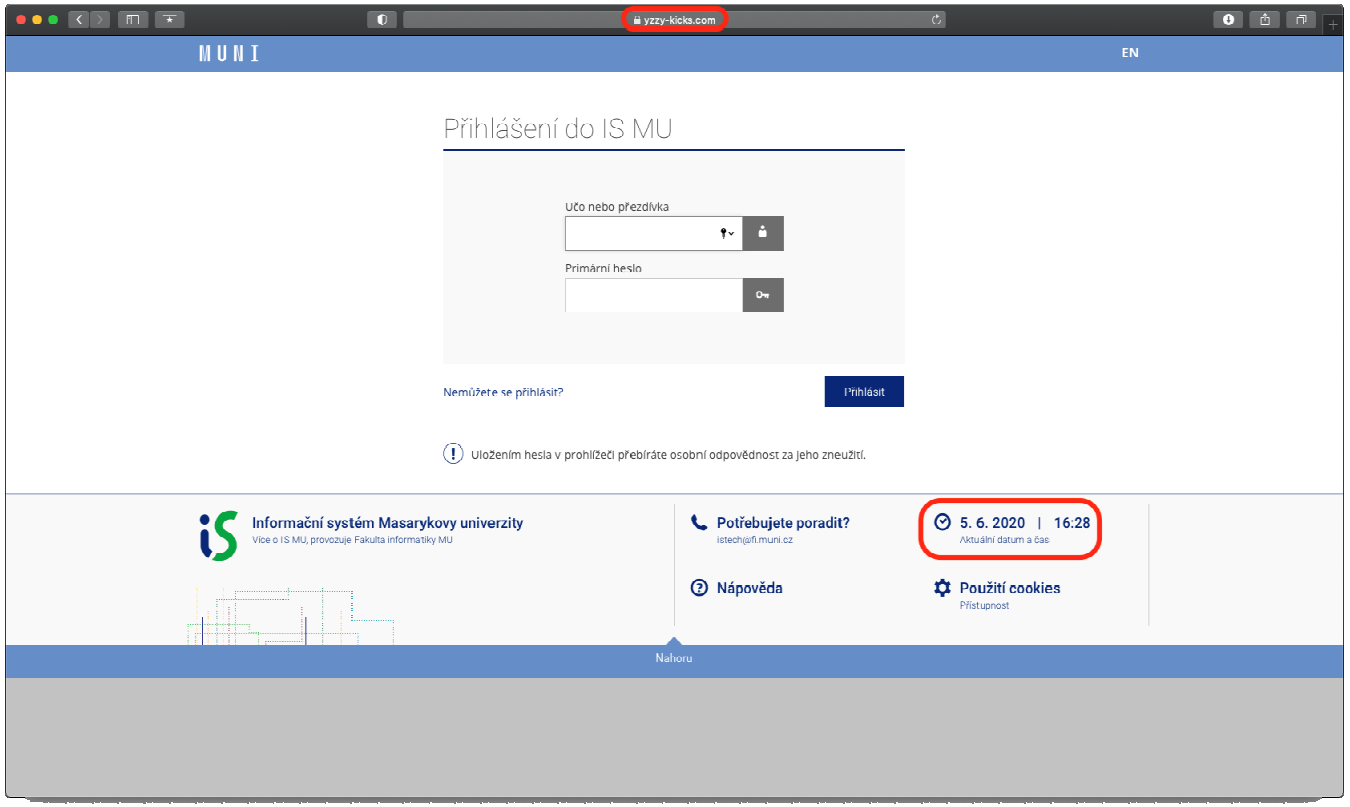
MUNI ICS

Spear-phishing – příklad

> Začátek přeposílané zprávy:
>
> Od: Masarykova univerzita Informační systém <alois.krobot@upol.cz>
> Předmět: 27. pondělí říjen 2020
> Datum: 27. října 2020 10:16:23 SEČ
> Komu: [redacted]
>
>
> 2 Nové oznámení týkající se vašich mezd 2020
>
> https://is.muni.cz/cz/Výplatní páska/2020/form.pdf <http://revuey25.revuex850.shakilislam.com/>
> (c) 2020 Masaryk Univerzita
>
> webmaster <mailto:webmaster-up@muni.cz>- <mailto:webmaster-up@muni.cz>u <mailto:webmaster-up@muni.cz>p <mailto:webmaster-up@muni.cz>@ <mailto:webmaster-up@muni.cz>m <mailto:webmaster-up@muni.cz>u <mailto:webmaster-up@muni.cz>n <mailto:webmaster-up@muni.cz>i <mailto:webmaster-up@muni.cz>. <mailto:webmaster-up@muni.cz>c <mailto:webmaster-up@muni.cz>z <mailto:webmaster-up@muni.cz>

MUNI ICS

Spear-phishing – příklad



MUNI ICS

MUNI
ICS

Sextortion

Sextortion

- Vydírání obětí **sexuálním kontextem** za pomoci relativně důvěryhodné zprávy
- Vyskytuje se i jako **forma kyberšikany**
- Častou cílovou skupinou jsou **dospívající lidé, vysoce postavené či spořádaní osoby**
- **Vyděračské e-maily obvykle**:
  - Bývají zasílány **masově** (plané výhrůžky)
  - Požadují poplatek relativně **malého množství peněz** (např. 200-250 USD)
  - Snaží se uživatele dostat do **časového stresu** (zaplať do 24-48 hodin)
  - Obsahují „jako důkaz“ **legitimní přihlašovací údaje** uživatele (typicky z nějakého úniku dat – např. Mall.cz)
- Výhružky se ale **mohou skutečně naplnit**, pokud útočník například pomocí Spyware odposlouchává zařízení nebo sleduje webkameru.

Sextortion – příklad

Ahoj!
Jsem členem mezinárodní hackerské skupiny.

Jak jste asi pravděpodobně uhodli, váš účet z domény@domain.com byl napaden, protože Poslal jsem vám e-mail z vašeho účtu.

V období od 5. července 2018 do 21. září 2018 jste byli infikováni virem, který jste vytvořili, prostřednictvím navštívených webových stránek pro dospělé.
Zatím máme přístup k vašim vzkazům, účtům sociálních médií a poslům.
Máme však úplné skládky těchto dat.

Jsme si vědomi svých malých a velkých tajemství ... jo, máte je.
Zaznamenali jsme a zaznamenávali vaše akce na pornografických webových stránkách. Váš vkus je tak divný, víte ..

Ale klíčovou věcí je, že jsme někdy zaznamenali vás s vaší webovou kamerou a synchronizovali nahrávky s tím, co jste sledovali!
Myslím, že nemáte zájem ukázat toto video svým přátelům, příbuzným a vašemu intimnímu ...

Přeneste 250$ do naší Bitcoin peněženky: 139XY4ZjWYqHMJvGCySuzXq7o6tGccKKrJ
Garantuji, že po tom budeme smazat všechny vaše "data": D

Po přečtení této zprávy se spustí časovač. Máte 48 hodin na zaplacení výše uvedené částky.

Vaše údaje budou vymazány po převodu peněz.
V opačném případě budou všechny vaše záznamy a videozáznamy automaticky zaslány všem vašim kontaktům, které jsou na vašem zařízení nalezeny v okamžiku infekce.

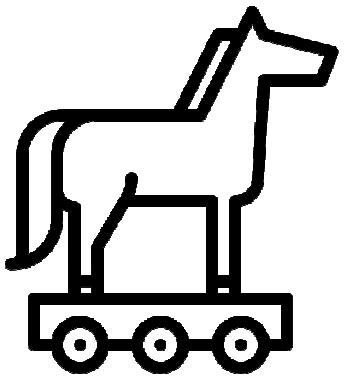
Měli byste vždy myslet na vaši bezpečnost. Doufáme, že vás tento případ naučí udržovat tajemství.
Opatruj se.

MUNI
ICS

Malware

Malware

- Škodlivý kód, který se šíří prostřednictvím bezpečnostních zranitelností v systémech, na kterých nebyly nainstalovány potřebné záplaty či aktualizace.
- Časté iniciální doručení za pomoci spear-phishingu, USB flash či Drive-by-download
- Základní typy malware:
  - Trojské koně
  - Ransomware
  - Spyware
  - Viry a červy
  - Backdoor
  - Downloadery



Malware

Hrozba (Emotet-Ostap)-Trickbot-Ryuk

1. Spear-phishing – iniciální vektor (neuhrazená pohledávka či faktura)
2. Emotet či Ostap – Downloader.JS (pomocí VBA maker v souborech)
3. Trickbot – malware (komunikace s C&C serverem)
4. Ryuk – ransomware (šifrování dat na disku)

- https://blog.iinfosec.com/ransomware-attack-analysis

Malware – příklad

Date: Fri, 3 Jan 2020 08:23:35 +0200
From: Valentina Aulisa <carolyn@digitalnews-online.com>
To: [redacted]
Subject: Pohledávky. Dôvodová správa.

Vážení,

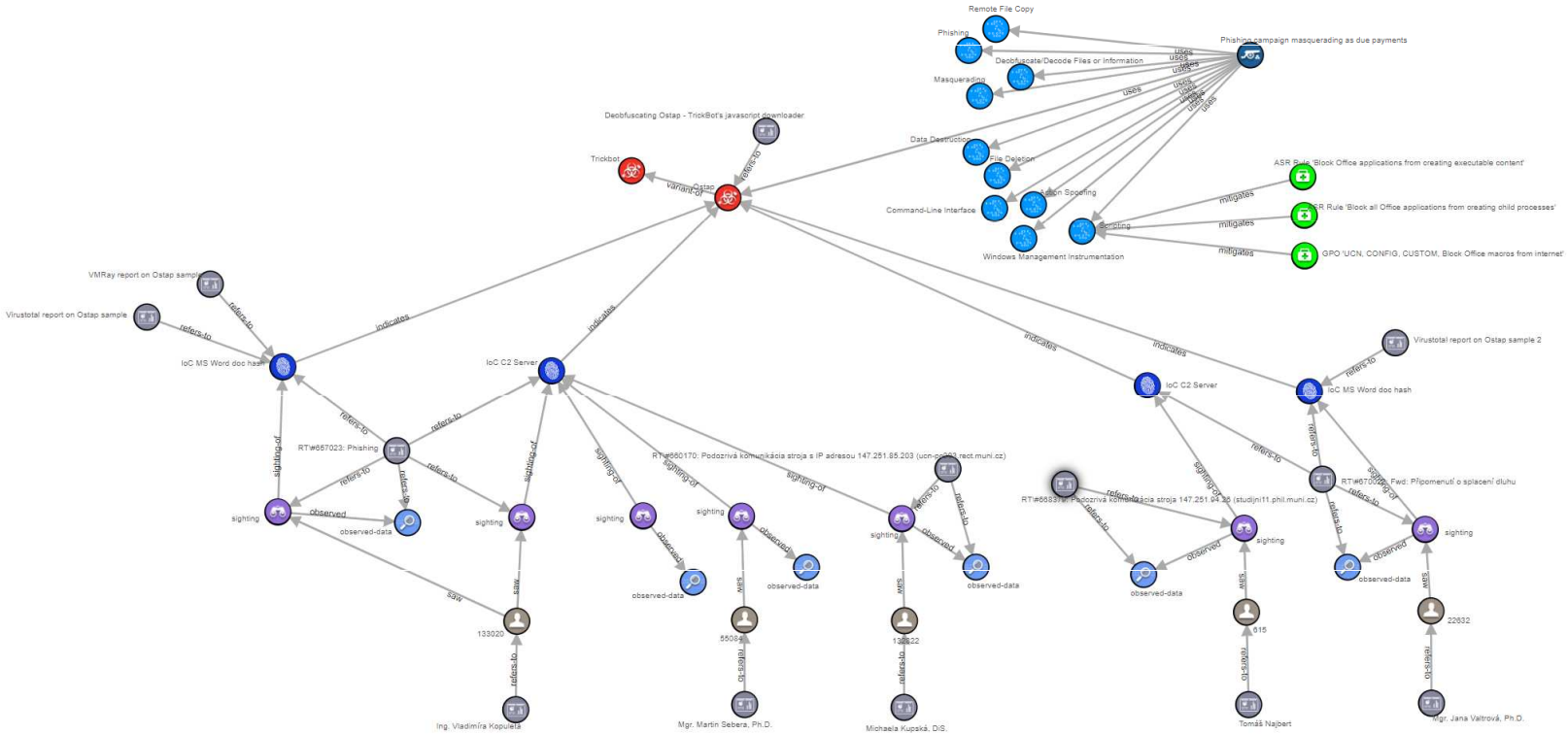
kontrolou naší účetní evidence jsme zjistili, že jste nám dosud neuhradili dlužnou částku ve výši 6.437,- Kč.

Současně vás tímto upozorňujeme, že pokud k úhradě uvedené částky na základě této písemné výzvy dobrovolně nedojde, případně se ani neozvete, a to obratem, za účelem návrhu akceptovatelného řešení této situace, jsme připraveni se domáhat uvedeného nároku právní cestou, především pak podáním žaloby k místně příslušnému soudu

Dôvodová správa v příloze (zahrnuje fakturu a smlouvu).

S pozdravem a přáním hezkého dne,
Valentina Aulisa
advokát/attorney at law
Opatovická 1633/8, Praha 1

Malware – formální popis útoku



MUNI ICS

MUNI
ICS

Ransomware

Ransomware

- Škodlivý SW určený k **zašifrování dat oběti s cílem požadovat výkupné**
- Dnes často v rámci útoků na **nemocnice nebo vysoké školy**
- Ve většině případů se jedná **čistě o formu businessu**
  - Útočníci chtějí vydělat peníze a poskytují k tomu i patřičné zázemí
- Lze použít i jako útok v rámci **nekalé soutěže** mezi konkurenčními firmami
- **Jen zřídka** se jedná o osobní typ útoku
- Zálohování pro obnovu dat **nemusí vždy stačit**
- Útočníci **vyhrožují zneužitím či prodejem** „tajemství“ z odcizených dat

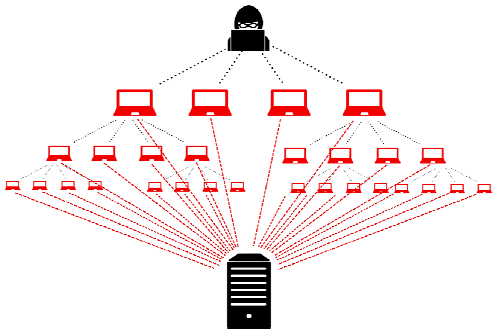
MUNI
ICS

Odepření služby (DDoS)

Odepření služby (DDoS)

- **Zahlcení cílového bodu** (služby či stroje) falešnými žádostmi, čímž dojde k **znemožnění vykonávání legitimní činnosti**
- Přetažení zařízení, služby či sítě vede **k omezení provozu**
- Legitimní uživatelé se tak **nemohou dostat** například na webovou stránku
- Typickou metodou **reflexe** (odražení) či **amplifikace** (zesílení)

- **Denial of Service attack (DoS)**
- **Distributed Denial of Service attack (DDoS)**



MUNI
ICS

Man-in-the-Middle

Man-in-the-Middle

- **Odposlouchávání komunikace** typicky v rámci počítačové sítě
  - Mezi uživatelem a aplikací, mezi dvěma uživateli, mezi dvěma službami
- Oblíbený způsob realizace za pomoci bezplatné veřejné WiFi sítě bez hesla
  - Správce (hacker) vidí všechen síťový provoz přihlášených uživatelů
- Útočníci rovněž využívají webových stránek šifrovaných protokolů (HTTPs)
- Sofistikované útoky pak počítají s „odstraněním“ šifrování (např. SSL Stripping)
  - Ještě před navázáním šifrovaného spojení
- Teoretická možnost „rozbíjet“ již ustanovené spojení, nicméně velmi výpočetně náročné
- Nicméně s TLS certifikátem jde samozřejmě všechno lépe (platí pro obě strany)

MUNI
ICS

Drive-by-download

Drive-by-download

- **Neúmyslné stažení** počítačového softwaru z internetu
  - Stahování, které uživatal autorizoval, aniž by si byl vědom důsledků
  - Jakékoli stažení, ke kterému dojde bez vědomí uživatele
- **Odkazy na různá úložiště** (Google Drive, Úschovna, RapidShare)
- Stažený soubor se **tváří jako legitimní SW** (často s překvapením)
- **Cracknuté či neoficiální** verze aplikací
- Většinou dokáže **odchytit antivirové řešení** (pokud jej nevypnete)

MUNI
ICS

Kyberkompas

Kurz základů informační bezpečnosti pro uživatele

Zdroj: https://security.muni.cz/cybercompass

Jak vytvořit z maličkostí účinnou obranu?

Hranice mezi vaším online a offline světem se stírá: tak proč volit pro zabezpečení dvojí metr? Je na čase dopřát všem digitálním zařízením adekvátní péči. Antiviry, zálohování, šifrování, zamykání a zavírání obrazovek probereme srozumitelně hned v první lekci.

ZABEZPEČENÍ ZAŘÍZENÍ

Jak dobře jsou střeženy vaše cennosti?

Jsou to právě hesla, za kterými se skrývají vaše (online) identity, cennosti a informace. Ve druhé lekci se naučíte vytvořit frázové heslo (nejsilnější, a přece nejsnazší na zapamatování), objevíte praktičnost správce hesel a zjistíte, jak se chovat k heslům tak, aby zůstala jen vaše.

HESLA

Jak se nenechat ošálit v kyberprostoru?

Člověk je omylný a je to naprosto v pořádku. V kyberprostoru se ale jedná o charakteristiku nejčastěji využívanou útočníky. Jak se ubránit manipulativním technikám tzv. sociálního inženýrství, jak spravovat digitální stopu a jak si snadno zašifrovat data, najdete ve třetí lekci.

SEBEOBRANA

Využíváte všechny výhody, které MUNI nabízí?

Masarykova univerzita poskytuje členům univerzity služby, za které by si jinak nemálo připlatili. Ve čtvrté lekci objevíte vychytávky Eduroamu, naučíte se bezpečně připojit i z kavárny, poslat opravdu soukromou zprávu nebo třeba chytře nasdílet výzkumná data.

BEZPEČNÁ KOMUNIKACE

Jak si poradit s bezpečnostním incidentem?

Útoky v digitálním světě nabývají čím dál větší rozmanitosti a promyšlenosti – neváhejte nahlásit sebemenší podezření či nesrovnalost. V páté lekci zjistíte, komu se ozvat, když se něco (možná) stalo a kdo konkrétně vám poradí na MUNI. Uživatel nemusí být nejslabším článkem řetězu!

HLÁŠENÍ INCIDENTŮ

Neloučíme se: tady totiž cesta nekončí

Je náročné začít přemýšlet o mnoha věcech úplně jinak. Pojďte si na závěr připomenout, co všechno jste se dozvěděli – a nechte se překvapit rozšiřujícími multimediálními materiály. Lekce je vhodná jako tahák, ke kterému se vrátíte, jakmile si v budoucnu nebudete něčím rychle jisti.

KYBERTAHÁK

Ochrana na úrovni uživatele

1. Mějte nainstalován antivirový program a udržujte jej aktualizovaný
2. Udržujte operační systém i aplikace aktuální
3. Vždy ověřujte adresu odesílatele zprávy a adresní řádek na webu (tzv. URL)
4. Neotvírejte e-maily a přílohy z podezřelých zdrojů
5. Vytvářejte silná hesla a změňte si všechny defaultní nebo opakovaně použitá hesla
6. Zrušte služby a účty, které se nepoužívají nebo už nejsou potřebné
7. Průběžně sledujte aktuální hrozby
8. Zálohujte a občas testujte zálohy
9. Hlašte bezpečnostní incidenty
10. Buďte kritičtí k tomu s čím se potkáte a pokud nevíte, ptejte se!

Ochrana na úrovni organizace

- CSIRT = Computer Security Incident Response Team
- Tým odborníků *nejen* na počítačovou bezpečnost
- Činnosti:
  - Reakce na kyberbezpečnostní události
  - **Koordinace** řešení kyberbezpečnostních incidentů
  - **Minimalizace** dopadů a škod
  - **Reportování** nadřazeným CSIRT týmům

CSIRT-MU

Naše mise

Masarykova univerzita je moderní vzdělávací instituce, pro niž je bezpečné kyberprostředí nezbytné. Naším cílem je zajistit, aby takové skutečně bylo. Toho dosahujeme výzkumem aktuálních hrozeb a možností jejich potlačení, stejně tak vzděláváním uživatelů a IT expertů.

Akademický CSIRT

Zajištění provozní bezpečnosti organizace

- Studenti a zaměstnanci univerzity
- IP adresy z rozsahů 147.251.0.0/16 a 2001:718:801::/48
- Doména muni.cz
- Významné informační systémy dle ZoKB

Inovace prostřednictvím VaV projektů

- Základní i aplikovaný výzkum (MŠMT, MV ČR, MO)
- Projekty s průmyslovými partnery (TA ČR)
- CRP projekty (MŠMT, MU)
- Ostatní (FR CESNET)

MUNI ICS

Poskytované kategorie služeb pro univerzitu

INFORMACE A VAROVÁNÍ

HLÁŠENÍ INCIDENTŮ

PENETRAČNÍ TESTOVÁNÍ

VZDĚLÁVÁNÍ SPRÁVCŮ

VZDĚLÁVÁNÍ UŽIVATELŮ

MUNI ICS

Přehled činností

- **Provoz certifikovaného bezpečnostního týmu CSIRT-MU (TF-CSIRT)**
  - Plnění povinností daných Zákonem o kybernetické bezpečnosti (ZoKB)
  - Poskytování součinnosti bezpečnostním složkám ČR (PČR, NCOZ, NÚKIB)
  - Spolupráce s národními a mezinárodními bezpečnostními týmy (CESNET-CERTS, CSIRT.CZ)
  - Spolupráce s CIT na jednotlivých fakultách
- **Penetrační testování univerzitních systémů**
  - V poslední době např. MUNI Pomáhá, JobCheckIN
- **Osvěta a vzdělávání univerzitních uživatelů a skupin**
  - Kyberkompas, kurzy U3V a CŽV, školení správců

MUNI ICS

Přehled dalších činností

- **Provoz zabezpečeného IS v režimu „Vyhrazené“**
  - Zákon č. 412/2005 Sb. „o ochraně utajovaných informací“
  - Umožňuje univerzitě ucházet se o projekty v režimu „Vyhrazené“
- **Údržba a rozvoj bezpečnostních nástrojů**
  - Každoroční investice ve výši několika mil. Kč
- **Výzkum a vývoj v oblasti kyberbezpečnosti**
  - Inovace řešeny v rámci projektů aplikovaného výzkumu (výstupy nasazovány do provozu)
    - Aktuálně jsme řešitelé tří H2020 projektů, tří projektů bezpečnostního výzkumu MV ČR, dvou projektů MŠMT a jednoho projektu TA ČR
  - Publikace za posledních 5 let: 2016: **11**, 2017: **19**, 2018: **23**, 2019: **29**, 2020: **35**

Co dělat v případě incidentu?

- Nepředpokládáme, že budete odborníky na kyberbezpečnost – **to je náš úkol**
- Pokud si nejste zcela jistí, vždy raději incident nahlašte – **budeme Vám vděční**
- Pište na e-mailovou adresu csirt@muni.cz nebo využijte formulář na webu csirt.muni.cz

1. Identifikujte se
2. Popište problém
3. Přiložte důkazy

→ NAHLÁSIT BEZPEČNOSTNÍ INCIDENT

MUNI ICS

Ochrana na úrovni CESNETu

- **CESNET – sdružení vysokých škol a AV ČR**
- Spravuje e-infrastrukturu pro přenos, zpracování a ukládání dat, spolupráci mezi uživateli a týmy
- Připojuje VVŠ a AV ČR k ostatní výzkumným sítím a „normálnímu“ internetu
- Provoz kyberbezpečnostního týmu CESNET-CERTS
- Ochrana na úrovni perimetru
  - Monitoring sítě, SIEM, detekce útoků, sdílení událostí, scrubbing centrum (ochrana před DDoS)
- Poskytování služby z pohledu NREN pro VVŠ
  - Eduroam, správa identit, certifikáty, Metacentrum, penetrační testování, dohledové centrum

Ochrana na úrovni státu

- **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)**
  - Ústřední správní orgán pro **kybernetickou bezpečnost** včetně ochrany **utajovaných informací** v oblasti informačních a komunikačních systémů **a kryptografické ochrany.**
  - Řídí se ZoKB (z. č. 181/2014) a VoKB (v. č. 82/2018)
  - Provozuje kyberbezpečnostního týmu GovCERT
  - Vyhodnocuje a ošetřuje aktuální rizika, vydání varování a definuje opatření
  - Koordinuje řešení KB incidentů hlášených z KII, ISZS a VIS
  - Provádí osvětovou a vzdělávací činnost

Chcete se dozvědět více?

- Stránky CSIRT-MU – https://csirt.muni.cz
- Bezpečnostní portál MUNI – https://security.muni.cz
- Kurz Kyberkompas
- Kurz GDPR
- Techniky sociálního inženýrství
- Projekt CRP-KYBER21

MUNI ICS

Témata esejí

- Kyberhygiena jako návyk člověka v 21.století
- Kyberbezpečnost a její vliv na jiné obory
- Kyberútoky - moderní hrozba dnešní společnosti
- Phishingové útoky - moderní hrozba dnešní společnosti

MUNI
ICS

Děkujeme za pozornost

MUNI
CSIRT-MU