Bezpečnost v IT

1. přednáška

Radek Janoštík

Univerzita Palackého v Olomouci

16. 2. 2024

Outline

- Úvod, organizační záležitosti
- Náplň předmětu
- Opakování
- Autentizace
- Legislativní okénko
- Sociální inženýrství
- Doporučená četba

Úvod

- Předmět (volně) navazuje na Počítačové sítě 1 a souvisí s Počítačové sítě 2
- Budeme předpokládat znalost témat z těchto předmětů
- Dvě hodiny týdně přednáška, bohužel není cvičení
- Doporučuji si projít cvičení z denního studia
- Probereme základní témata s počítačové bezpečnosti

Konzultace, kontakt

- Email: radek.janostik@upol.cz
- Pracovna: 5.073
- Telefon: 585 634 711
- Web: `https://apollo.inf.upol.cz/~janostik/`
- Konzultace: Pátek 8:00 – 9:30 nebo dohodou

Doporučená literatura (1 / 2)

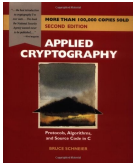
- William Stallings. *Network Security Essentials: Applications and Standards* (6th Edition). Pearson, 2016. ISBN: 1-292-15485-3, 978-1-292-15485-5.

- Dostálek L. a kolektiv. *Velký průvodce protokoly TCP/IP: Bezpečnost* (2. aktualizované vydání). Computer Press, 2003. ISBN 807226849X.

Doporučená literatura (2 / 2)

- Singh S. 2003. *Kniha kódů a šifer – Tajná komunikace od starého Egypta po kvantovou kryptografii*. Dokořán.

- Schneier B. *Applied Cryptography Second Edition*. John Wiley & Sons, 1996. ISBN 0-471-12845-7.



Jízdní řád)

- 1. Úvodní hodina, opakování, autentizace, legislativa, sociální inženýrství,
- 2. Úvod do kryptografie, symetrické a asymetrické šifry, DES a AES, RSA
- 3. Public Key Infrastructure, Digitální podpis, časová razítka, zabezpečení emailu
- 4. Zabezpečení aplikací, chyby HW, buffer overflow, sandboxing, viry, antiviry, malware, ransomware, Bezpečnost webových aplikací
- 5. Bezpečnost síťových technologií (Ethernet, WiFi)
- 6. Bezpečnost TCP/IP: Tunelování, VPN, Tor, blockchain jako struktura pro nezměnitelná data

Zkouška

- Zkouška bude ústní formou
- Dvě otázky
  - 1. „do hloubky“ (komplexnější téma)
  - 2. „přehledová“ (vedlejší téma, přehledově, základní principy)
- Otázky z probraných okruhů + základní otázky z KMI/POS 1 (budou konkretizovány)
- $\approx$ 20 minut příprava $\Rightarrow$ ústní zkoušení, doptávání, diskuze
- Předtermín v zápočtovém týdnu

Anketa + prezenčka

Anketa + prezenčka

- Kdo se aktivně stará o nějakou síť?

Anketa + prezenčka

- Kdo se aktivně stará o nějakou síť? Jak velkou?

Anketa + prezenčka

- Kdo se aktivně stará o nějakou síť? Jak velkou?
- Kdo v posledním půlroce použil nějaké diagnostické síťové nástroje mimo výuku?

Anketa + prezenčka

- Kdo se aktivně stará o nějakou síť? Jak velkou?
- Kdo v posledním půlroce použil nějaké diagnostické síťové nástroje mimo výuku?
- Spravujete nějaký server? Webovou aplikaci? Jaký/jakou?

Anketa + prezenčka

- Kdo se aktivně stará o nějakou síť? Jak velkou?
- Kdo v posledním půlroce použil nějaké diagnostické síťové nástroje mimo výuku?
- Spravujete nějaký server? Webovou aplikaci? Jaký/jakou?
- Kdo průběžně sleduje trendy/novinky počítačové bezpečnosti?

Anketa + prezenčka

- Kdo se aktivně stará o nějakou síť? Jak velkou?
- Kdo v posledním půlroce použil nějaké diagnostické síťové nástroje mimo výuku?
- Spravujete nějaký server? Webovou aplikaci? Jaký/jakou?
- Kdo průběžně sleduje trendy/novinky počítačové bezpečnosti?
- „Zatopil“ někomu nějaký vir/ransomware?

Anketa + prezenčka

- Kdo se aktivně stará o nějakou síť? Jak velkou?
- Kdo v posledním půlroce použil nějaké diagnostické síťové nástroje mimo výuku?
- Spravujete nějaký server? Webovou aplikaci? Jaký/jakou?
- Kdo průběžně sleduje trendy/novinky počítačové bezpečnosti?
- „Zatopil“ někomu nějaký vir/ransomware?
- Stal se někdo obětí phishingu? Úniku dat?

Anketa + prezenčka

- Kdo se aktivně stará o nějakou síť? Jak velkou?
- Kdo v posledním půlroce použil nějaké diagnostické síťové nástroje mimo výuku?
- Spravujete nějaký server? Webovou aplikaci? Jaký/jakou?
- Kdo průběžně sleduje trendy/novinky počítačové bezpečnosti?
- „Zatopil“ někomu nějaký vir/ransomware?
- Stal se někdo obětí phishingu? Úniku dat?
- Přizná se někdo k *„ne zrovna etickému/legálnímu chování“* na síti/v systémech?

Opakování

Opakování – co byste měli znát

- Historie rozvoje počítačů, sítí
  - Počátky komunikace (přenos pomocí médií, první sítě – spojované okruhy, uchová stav)
  - Později nespojované sítě - přepínání paketů
  - Původně téměř vůbec nebyl kladen důraz na bezpečnost. Spíše jen na funkčnost
- Pro komunikaci musíme znát/umět
  - Formát posílaných zpráv
  - Jak určit aplikaci, které je zpráva určena
  - Jak určit počítač, kam má zpráva dorazit
  - Kudy má zpráva na počítač dorazit
  - Jak reálně data přenést
  - Čím ta data přenést
- $\Rightarrow$ Abstraktní model komunikace $\Rightarrow$ konkrétní implementace

Transmission Control Protocol/Internet Protocol (TCP/IP)

- Používaný model v síti Internet
- 4vrstvá architektura (aplikační, transportní, síťová, síťového rozhraní)
- Jednotlivé vrstvy definovány ve volně dostupných „standardech“ *Request for Comments*
- `https://www.rfc-editor.org/standards`
- Protokoly = soubory přesných pravidel, podle kterých probíhá komunikace
- Původně žádný důraz na bezpečnost, byly možné (dnes již) triviální útoky
- Postupně dodány bezpečnostní mechanismy(fungující se starými) a nové protokoly

TCP/IP rychlé opakování

- Co to znamená, že počítač má IP adresu `158.194.92.7` a masku `255.255.255.0`?

TCP/IP rychlé opakování

- Co to znamená, že počítač má IP adresu `158.194.92.7` a masku `255.255.255.0`?
- Aplikace na tomto počítači chce komunikovat se serverem s doménovým jménem *root.cz*, co vše potřeba udělat?

TCP/IP rychlé opakování

- Co to znamená, že počítač má IP adresu `158.194.92.7` a masku `255.255.255.0`?
- Aplikace na tomto počítači chce komunikovat se serverem s doménovým jménem *root.cz*, co vše potřeba udělat?
- Jak operační systém zjistí, jakou linkovou adresu má brána `158.194.92.1`

TCP/IP rychlé opakování

- Co to znamená, že počítač má IP adresu `158.194.92.7` a masku `255.255.255.0`?
- Aplikace na tomto počítači chce komunikovat se serverem s doménovým jménem *root.cz*, co vše potřeba udělat?
- Jak operační systém zjistí, jakou linkovou adresu má brána `158.194.92.1`
- Jak je možné, že stroj *ts.inf.upol,cz* neodpovídá na `ping`, ale vzdálená plocha funguje?

TCP/IP rychlé opakování

- Co to znamená, že počítač má IP adresu `158.194.92.7` a masku `255.255.255.0`?
- Aplikace na tomto počítači chce komunikovat se serverem s doménovým jménem *root.cz*, co vše potřeba udělat?
- Jak operační systém zjistí, jakou linkovou adresu má brána `158.194.92.1`
- Jak je možné, že stroj *ts.inf.upol,cz* neodpovídá na `ping`, ale vzdálená plocha funguje?
- Jak probíhá navazování spojení v protokolu UDP?

TCP/IP rychlé opakování

- Co to znamená, že počítač má IP adresu `158.194.92.7` a masku `255.255.255.0`?
- Aplikace na tomto počítači chce komunikovat se serverem s doménovým jménem *root.cz*, co vše potřeba udělat?
- Jak operační systém zjistí, jakou linkovou adresu má brána `158.194.92.1`
- Jak je možné, že stroj *ts.inf.upol,cz* neodpovídá na `ping`, ale vzdálená plocha funguje?
- Jak probíhá navazování spojení v protokolu UDP?
- Může počítač **A** připojený do stejného switche jako počítače **B** a **C** odposlouchávat komunikaci mezi počítačem **B** a **C**? Proč?

TCP/IP rychlé opakování

- Co to znamená, že počítač má IP adresu `158.194.92.7` a masku `255.255.255.0`?
- Aplikace na tomto počítači chce komunikovat se serverem s doménovým jménem *root.cz*, co vše potřeba udělat?
- Jak operační systém zjistí, jakou linkovou adresu má brána `158.194.92.1`
- Jak je možné, že stroj *ts.inf.upol,cz* neodpovídá na `ping`, ale vzdálená plocha funguje?
- Jak probíhá navazování spojení v protokolu UDP?
- Může počítač **A** připojený do stejného switche jako počítače **B** a **C** odposlouchávat komunikaci mezi počítačem **B** a **C**? Proč?
- Co je to veřejná IP adresa?

TCP/IP rychlé opakování

- Co to znamená, že počítač má IP adresu `158.194.92.7` a masku `255.255.255.0`?
- Aplikace na tomto počítači chce komunikovat se serverem s doménovým jménem *root.cz*, co vše potřeba udělat?
- Jak operační systém zjistí, jakou linkovou adresu má brána `158.194.92.1`
- Jak je možné, že stroj *ts.inf.upol,cz* neodpovídá na `ping`, ale vzdálená plocha funguje?
- Jak probíhá navazování spojení v protokolu UDP?
- Může počítač **A** připojený do stejného switche jako počítače **B** a **C** odposlouchávat komunikaci mezi počítačem **B** a **C**? Proč?
- Co je to veřejná IP adresa? Jak poznám, že ji mám?

TCP/IP rychlé opakování

- Co to znamená, že počítač má IP adresu `158.194.92.7` a masku `255.255.255.0`?
- Aplikace na tomto počítači chce komunikovat se serverem s doménovým jménem *root.cz*, co vše potřeba udělat?
- Jak operační systém zjistí, jakou linkovou adresu má brána `158.194.92.1`
- Jak je možné, že stroj *ts.inf.upol,cz* neodpovídá na `ping`, ale vzdálená plocha funguje?
- Jak probíhá navazování spojení v protokolu UDP?
- Může počítač **A** připojený do stejného switche jako počítače **B** a **C** odposlouchávat komunikaci mezi počítačem **B** a **C**? Proč?
- Co je to veřejná IP adresa? Jak poznám, že ji mám? Kdo ji má?

Autentizace uživatele

Autentizace uživatele

- Proces ověření uživatele(/počítače) – uživatel (nějak) prokazuje, že je to skutečně on
- Autorizace = udělení konkrétní práv uživateli po jeho autentizaci
- Základní způsoby:
  - Uživatel zná něco (pseudo) unikátního – např. heslo, URL s hashem (ověření emailu)
  - Uživatel má něco unikátního – soukromý klíč, telefon, přístup k emailu
  - Biometrika uživatele (Je možná „biometrika“ počítače/aplikace?)

Autentizace uživatele

- Proces ověření uživatele(/počítače) – uživatel (nějak) prokazuje, že je to skutečně on
- Autorizace = udělení konkrétní práv uživateli po jeho autentizaci
- Základní způsoby:
  - Uživatel zná něco (pseudo) unikátního – např. heslo, URL s hashem (ověření emailu)
  - Uživatel má něco unikátního – soukromý klíč, telefon, přístup k emailu
  - Biometrika uživatele (Je možná „biometrika“ počítače/aplikace?)
- Příklad z reálného světa
  - Policista vás legitimuje (uvědomit si kroky, čemu věří?)
  - Nárok na slevu v hromadné dopravě

Autentizace heslem

- Heslo = tajná sekvence znaků, kterou by měl znát pouze uživatel
  - Co provozovatel služby? Musí znát heslo pro ověření správnosti?
- Co je to silné heslo?

Autentizace heslem

- Heslo = tajná sekvence znaků, kterou by měl znát pouze uživatel
  - Co provozovatel služby? Musí znát heslo pro ověření správnosti?
- Co je to silné heslo?
- Které heslo je silnější: `Uj|k25.xa` nebo `VceraJsemMelNaObedVeproZelo`

Autentizace heslem

- Heslo = tajná sekvence znaků, kterou by měl znát pouze uživatel
  - Co provozovatel služby? Musí znát heslo pro ověření správnosti?
- Co je to silné heslo?
- Které heslo je silnější: `Uj|k25.xa` nebo `VceraJsemMelNaObedVeproZelo`
- Které si snadněji zapamatujete?

Autentizace heslem

- Heslo = tajná sekvence znaků, kterou by měl znát pouze uživatel
  - Co provozovatel služby? Musí znát heslo pro ověření správnosti?
- Co je to silné heslo?
- Které heslo je silnější: `Uj|k25.xa` nebo `VceraJsemMelNaObedVeproZelo`
- Které si snadněji zapamatujete?
- Správci hesel a jejich bezpečnost
- Ve starších aplikačních protokolech TCP/IP problémy s přenášením hesel v otevřené podobě
  - Telnet
  - HTTP basic auth
  - FTP

Jednorázová hesla

- Podaří-li se nám získat uživatelovo heslo (odposlech, přečtení z papírku na monitoru, ...) můžeme jej použít kolikrát chceme, dokud si jej uživatel nezmění $\Rightarrow$ problém
- Co kdyby heslo platilo jenom jednou, při další autentizaci by platilo jiné?
  - Jak neustále měnit?
  - Kdo by si to měl pamatovat?
  - Jak to zajistit?

Jednorázová hesla

- Podaří-li se nám získat uživatelovo heslo (odposlech, přečtení z papírku na monitoru, ...) můžeme jej použít kolikrát chceme, dokud si jej uživatel nezmění $\Rightarrow$ problém
- Co kdyby heslo platilo jenom jednou, při další autentizaci by platilo jiné?
  - Jak neustále měnit?
  - Kdo by si to měl pamatovat?
  - Jak to zajistit?
- Překvapivě to není neřešitelný problém
  - Seznam jednorázových hesel (distribuce?)
  - Rekurentní algoritmus (S/KEY, OTP)
  - Jednorázové heslo jiným kanálem (SMS, email, telefon, ...)

Rekurentní algoritmus

- Mějme nějakou *jednosměrnou* funkci f
  - Je *velmi snadné* vypočítat $f(x)$
  - Je *velmi obtížné* najít takové y, že $y = f(x)$
- Často jsou používány hashovací funkce (více později v kurzu)
- $f^n(x)$ značí n-krát použití funkce f s počátečním řetězcem x
- Např. $f^4(x) = f(f(f(f(x))))$

Rekurentní algoritmus

- Mějme nějakou *jednosměrnou* funkci f
  - Je *velmi snadné* vypočítat $f(x)$
  - Je *velmi obtížné* najít takové y, že $y = f(x)$
- Často jsou používány hashovací funkce (více později v kurzu)
- $f^n(x)$ značí n-krát použití funkce f s počátečním řetězcem x
- Např. $f^4(x) = f(f(f(f(x))))$
- Inicializace
  - Uživatel si zvolí tajný řetězec *seed*
  - Uživatel si zvolí číslo n a spočítá $f^n(seed)$ a dvojici $\langle n, f^n(seed)\rangle$ pošle autentizující aplikaci

Rekurentní algoritmus

- Mějme nějakou *jednosměrnou* funkci f
  - Je *velmi snadné* vypočítat $f(x)$
  - Je *velmi obtížné* najít takové y, že $y = f(x)$
- Často jsou používány hashovací funkce (více později v kurzu)
- $f^n(x)$ značí n-krát použití funkce f s počátečním řetězcem x
- Např. $f^4(x) = f(f(f(f(x))))$
- Inicializace
  - Uživatel si zvolí tajný řetězec *seed*
  - Uživatel si zvolí číslo n a spočítá $f^n(seed)$ a dvojici $\langle n, f^n(seed)\rangle$ pošle autentizující aplikaci
- Autentizace
  - Uživatel zašle serveru jméno
  - Server nalezne v databázi současné n a odešle uživateli $n-1$
  - Uživatel spočítá $f^{n-1}(seed)$ a pošle jej serveru
  - Server spočítá $f(f^{n-1}(seed))$ a ověří, zda se rovná f^n z databáze (a sníží n a $f(n)$ v DB)
- Příklad na tabuli (server nezná *seed*!)

S/KEY a OTP

- S/KEY – konkrétní implementace rekurentního algoritmu – RFC-1760
  - Umožňuje použít pouze hashovací funkcí MD4
  - Dělí její výstup na poloviny, poté XOR $\Rightarrow$ 8 bajtů
  - Parametry definuje server (číslo n + sůl). Klient může mít stejný *seed* pro více serverů
  - MD4 se již dlouho nepovažuje za kryptograficky bezpečnou (lze snadno invertovat)

S/KEY a OTP

- S/KEY – konkrétní implementace rekurentního algoritmu – RFC-1760
  - Umožňuje použít pouze hashovací funkcí MD4
  - Dělí její výstup na poloviny, poté XOR $\Rightarrow$ 8 bajtů
  - Parametry definuje server (číslo n + sůl). Klient může mít stejný *seed* pro více serverů
  - MD4 se již dlouho nepovažuje za kryptograficky bezpečnou (lze snadno invertovat)
- OTP (One Time Password) – RFC-2289
  - Definuje formát zpráv pro autentizační komunikaci
  - Rozšiřuje S/KEY o MD5 a SHA1
  - Povinná je pouze MD5 (již taky není bezpečná)

Legislativa – průnik do počítačových systémů

Legislativa – průnik do počítačových systémů

- Průnik do počítačových systémů ošetřuje Trestní zákoník - Zákon č. 40/2009 Sb. §230-232 `https://www.zakonyprolidi.cz/cs/2009-40`
- Citace: „(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“
  - Už samotné přihlášení do systému, kde „nemáme co dělat“ je porušením zákona
  - Odstavce 2-5 pouze zvyšují trest na základě toho jakou škodu jste způsobili
  - Např. prolomení hesla na WiFi(WEP) a její používání je porušením §231 odst. 1 písm. b)
- §231 Specifikuje tresty podle toho co s získanými hesly/postupem uděláte
- §232 Ošetřuje škody způsobené z nedbalosti („ukliknete se v práci na produkčním serveru“, smažete privátní klíče, . . .)

GDPR a osobní údaje

- GDPR = Obecné nařízení o ochraně osobních údajů (Nařízení Evropského parlamentu)
- ČR měla ochranu osobních údajů podchycenou i dříve
- Kdo někdy četl plné znění?
  `https://www.uoou.cz/uplne-zneni-gdpr/ds-6607/archiv=1&p1=3938`
- Článek 4, odst. 1: „osobními údaji“ **veškeré** informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“

GDPR a osobní údaje

- Je IP adresa osobním údajem?

GDPR a osobní údaje

- Je IP adresa osobním údajem?
  - Na internetu spousta mýtů

GDPR a osobní údaje

- Je IP adresa osobním údajem?
  - Na internetu spousta mýtů
  - Samotná nikoliv
  - V kombinaci s historií procházených webů (cookies) může

GDPR a osobní údaje

- Je IP adresa osobním údajem?
  - Na internetu spousta mýtů
  - Samotná nikoliv
  - V kombinaci s historií procházených webů (cookies) může
- Je emailová adresa osobním údajem?

GDPR a osobní údaje

- Je IP adresa osobním údajem?
  - Na internetu spousta mýtů
  - Samotná nikoliv
  - V kombinaci s historií procházených webů (cookies) může
- Je emailová adresa osobním údajem?
  - Firemní, aktuální – radek.janostik@upol.cz – ano
  - Freemail karel99@seznam.cz (samotná) nikoliv

GDPR a osobní údaje

- Je IP adresa osobním údajem?
  - Na internetu spousta mýtů
  - Samotná nikoliv
  - V kombinaci s historií procházených webů (cookies) může
- Je emailová adresa osobním údajem?
  - Firemní, aktuální – radek.janostik@upol.cz – ano
  - Freemail karel99@seznam.cz (samotná) nikoliv
- Je kompletní poštovní adresa OÚ?

GDPR a osobní údaje

- Je IP adresa osobním údajem?
  - Na internetu spousta mýtů
  - Samotná nikoliv
  - V kombinaci s historií procházených webů (cookies) může
- Je emailová adresa osobním údajem?
  - Firemní, aktuální – radek.janostik@upol.cz – ano
  - Freemail karel99@seznam.cz (samotná) nikoliv
- Je kompletní poštovní adresa OÚ?
  - Ano

GDPR a osobní údaje

- Je IP adresa osobním údajem?
  - Na internetu spousta mýtů
  - Samotná nikoliv
  - V kombinaci s historií procházených webů (cookies) může
- Je emailová adresa osobním údajem?
  - Firemní, aktuální – radek.janostik@upol.cz – ano
  - Freemail karel99@seznam.cz (samotná) nikoliv
- Je kompletní poštovní adresa OÚ?
  - Ano
- $\Rightarrow$ každý kdo zpracovává osobní údaje by měl k tomu mít souhlas s uživatelem
- Zaměstnanci podepsanou mlčenlivost
- Spousta jemných nuancí, co, kdo, jak dlouho, jestli vůbec $\Rightarrow$ právník
- Zajímavé čtení o informačních systémech:
  `https://www.uoou.cz/informacni-systemy/d-6136/p1=3938`

Sociální inženýrství

- „Social engineering bypasses all technologies, including firewalls“, Kevin Mitnick
- $\Rightarrow$ Útok na nejslabší článek systémů (jaký?)

Sociální inženýrství

- „Social engineering bypasses all technologies, including firewalls“, Kevin Mitnick
- $\Rightarrow$ Útok na nejslabší článek systémů (jaký?) lidský faktor

Sociální inženýrství

- „Social engineering bypasses all technologies, including firewalls“, Kevin Mitnick
- $\Rightarrow$ Útok na nejslabší článek systémů (jaký?) lidský faktor
- = Využití psychologických triků a forem manipulace k přesvědčení uživatelů k
  - vyzrazení důvěrných informací (a jejich využití později)
  - udělení přístupu (fyzicky, oprávnění, . . .)
  - vyplacení peněz
  - . . .

Sociální inženýrství

- „Social engineering bypasses all technologies, including firewalls“, Kevin Mitnick
- $\Rightarrow$ Útok na nejslabší článek systémů (jaký?) lidský faktor
- = Využití psychologických triků a forem manipulace k přesvědčení uživatelů k
  - vyzrazení důvěrných informací (a jejich využití později)
  - udělení přístupu (fyzicky, oprávnění, . . .)
  - vyplacení peněz
  - . . .
- Využití částečné znalosti zabezpečení systému k přesvědčení
  - Podvodné emaily, telefonáty: „Ahoj tady Karel z oddělení cyber security, ještě se k mě nedostalo nové heslo, minulý měsíc bylo *StudujUp2022*, prosím tě, jaké je to nové?“
  - Útok na naléhavost, „převleky“, falešné vizitky, moderní plášť neviditelnosti, . . .

Sociální inženýrství

- „Social engineering bypasses all technologies, including firewalls“, Kevin Mitnick
- $\Rightarrow$ Útok na nejslabší článek systémů (jaký?) lidský faktor
- $=$ Využití psychologických triků a forem manipulace k přesvědčení uživatelů k
  - vyzrazení důvěrných informací (a jejich využití později)
  - udělení přístupu (fyzicky, oprávnění, . . .)
  - vyplacení peněz
  - . . .
- Využití částečné znalosti zabezpečení systému k přesvědčení
  - Podvodné emaily, telefonáty: „Ahoj tady Karel z oddělení cyber security, ještě se k mě nedostalo nové heslo, minulý měsíc bylo *StudujUp2022*, prosím tě, jaké je to nové?“
  - Útok na naléhavost, „převleky“, falešné vizitky, moderní plášť neviditelnosti, . . .
- Vše až překvapivě účinné

Sociální inženýrství – Kevin Mitnick (1963 – 2023)

- Asi nejznámější sociální inženýr a hacker
- Dokázal se nabourat do desítek sociálně technických systémů
  - Získal citlivé informace
  - Zničil některá data
  - Osobní obohacení

Sociální inženýrství – Kevin Mitnick (1963 – 2023)

- Asi nejznámější sociální inženýr a hacker
- Dokázal se nabourat do desítek sociálně technických systémů
  - Získal citlivé informace
  - Zničil některá data
  - Osobní obohacení
- První „sociální“ útok ve svých 12letech (manipulace s jízdenkami MHD)
- V 16letech průnik do systémů DEC
- Kombinace sociálního inženýrství a technických a hackerských metod
- Dopaden a zatčen v roce 1993 (zajímavý proces)

Sociální inženýrství – Kevin Mitnick (1963 – 2023)

- Asi nejznámější sociální inženýr a hacker
- Dokázal se nabourat do desítek sociálně technických systémů
  - Získal citlivé informace
  - Zničil některá data
  - Osobní obohacení
- První „sociální“ útok ve svých 12letech (manipulace s jízdenkami MHD)
- V 16letech průnik do systémů DEC
- Kombinace sociálního inženýrství a technických a hackerských metod
- Dopaden a zatčen v roce 1993 (zajímavý proces)
- Po propuštění mu byla na 3 roky zakázána jakákoliv (moderní) komunikace kromě pevné linky

Sociální inženýrství – Kevin Mitnick (1963 – 2023)

- Asi nejznámější sociální inženýr a hacker
- Dokázal se nabourat do desítek sociálně technických systémů
  - Získal citlivé informace
  - Zničil některá data
  - Osobní obohacení
- První „sociální“ útok ve svých 12letech (manipulace s jízdenkami MHD)
- V 16letech průnik do systémů DEC
- Kombinace sociálního inženýrství a technických a hackerských metod
- Dopaden a zatčen v roce 1993 (zajímavý proces)
- Po propuštění mu byla na 3 roky zakázána jakákoliv (moderní) komunikace kromě pevné linky
- Stal se konzultantem kyberbezpečnosti
- Napsal několik knih (doporučuji)

Sociální inženýrství – Frank Abagnale Jr.

- Známý filmem *Chyť mě, když to dokážeš* CSFD
- Je třeba představovat?

Sociální inženýrství – Frank Abagnale Jr.

- Známý filmem *Chyť mě, když to dokážeš* CSFD
- Je třeba představovat?
- $\Rightarrow$ Funguje sociální inženýrství ještě dnes?
- Podařil se někomu nějaký (neškodný) „kousek“?

Doporučená literatura (1/2)

- Opakování z počítačových sítí
  - Kabelová A., Dostálek L. Velký průvodce protokoly TCP/IP a systémem DNS (5. vydání). Computer Press, 2008.
- Autentizace, autorizace
  - Dostálek L. a kolektiv. Velký průvodce protokoly TCP/IP: Bezpečnost (2. aktualizované vydání). Computer Press, 2003. ISBN 807226849X (kap. 4)
- Mitnick K. , Simon W.L. Umění klamu. Helion, 2003. ISBN 83-7361-210-6

Doporučená literatura (2/2)

- Trestní zákoník – Zákon č. 40/2009 Sb.
  - § 230 – Neoprávněný přístup k počítačovému systému a nosiči informací
  - § 231 – Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
  - § 232 – Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
  - Některé věci mohou být ošetřeny zákonem O elektronických komunikacích, OOÚ, Autorský zákon, ...
  - Ščerba Filip a kolektiv. Trestní zákoník. Komentář (2 svazky). C.H.Beck, 2020. ISBN 978-80-7400-807-8 `https://library.upol.cz/arl-upol/cs/detail-upol_us_cat-0321234-Trestni-zakonik/?disprec=7&iset=2`
- GDPR, osobní údaje
  - Zákon č. 110/2019 Sb – O zpracování osobních údajů
  - `https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_cs`