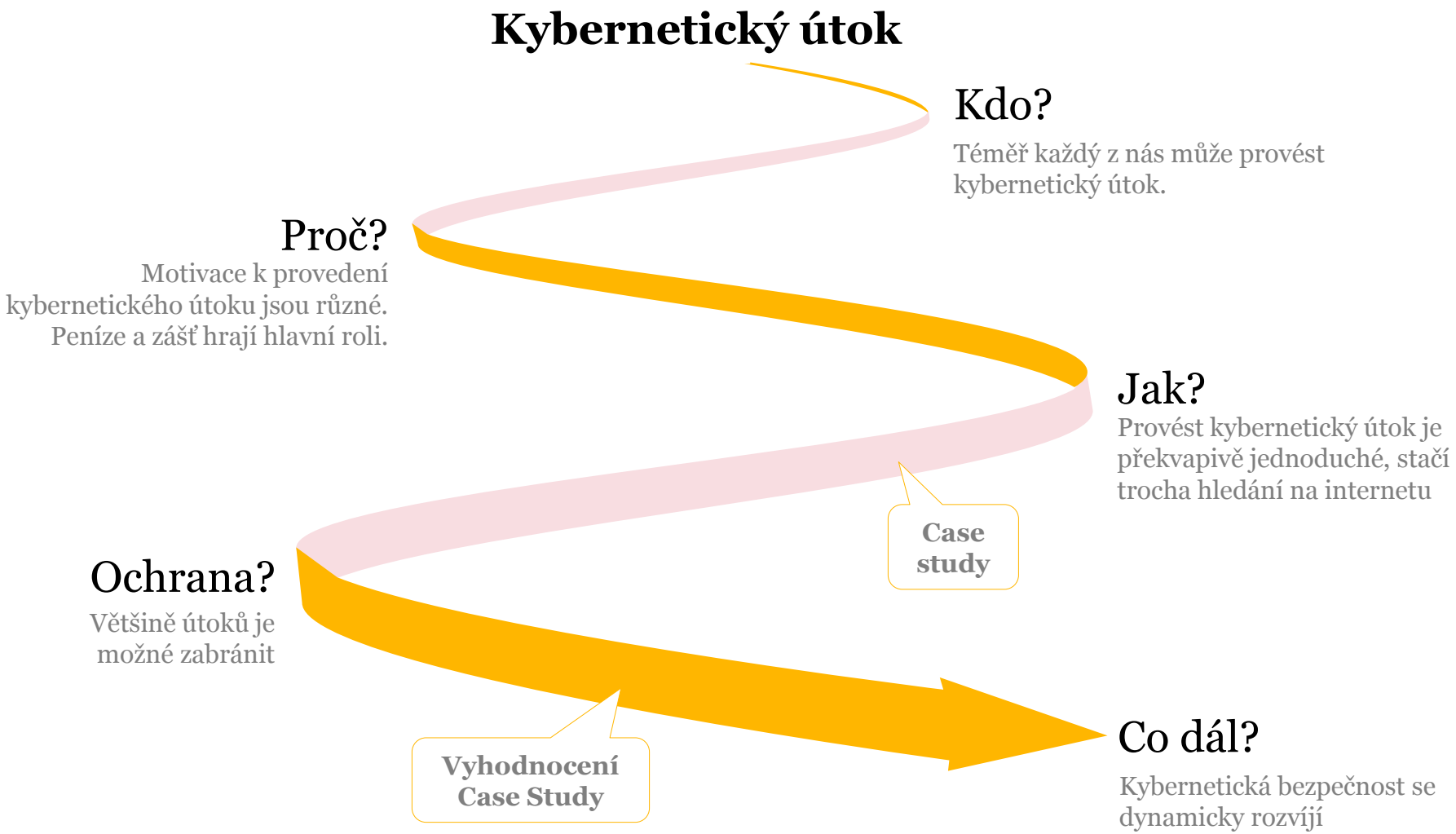
www.pwc.cz/ras

IT bezpečnost

Michal Čábela

pwc

Co nás čeká


Kybernetický útok
Kdo?
Téměř každý z nás může provést kybernetický útok.
Proč?
Motivace k provedení kybernetického útoku jsou různé. Peníze a zášť hrají hlavní roli.
Jak?
Provést kybernetický útok je překvapivě jednoduché, stačí trocha hledání na internetu
Case study
Ochrana?
Většině útoků je možné zabránit
Vyhodnocení Case Study
Co dál?
Kybernetická bezpečnost se dynamicky rozvíjí

Kybernetický útok

Příklady známých kybernetických útoků:

Stuxnet (2007 / 2008), Irán

Vysoká pec (2014), Německo

Jeep Cherokee (2015), USA

Ropne plosiny (2015), Severní moře

Varná konvice (2015), USA

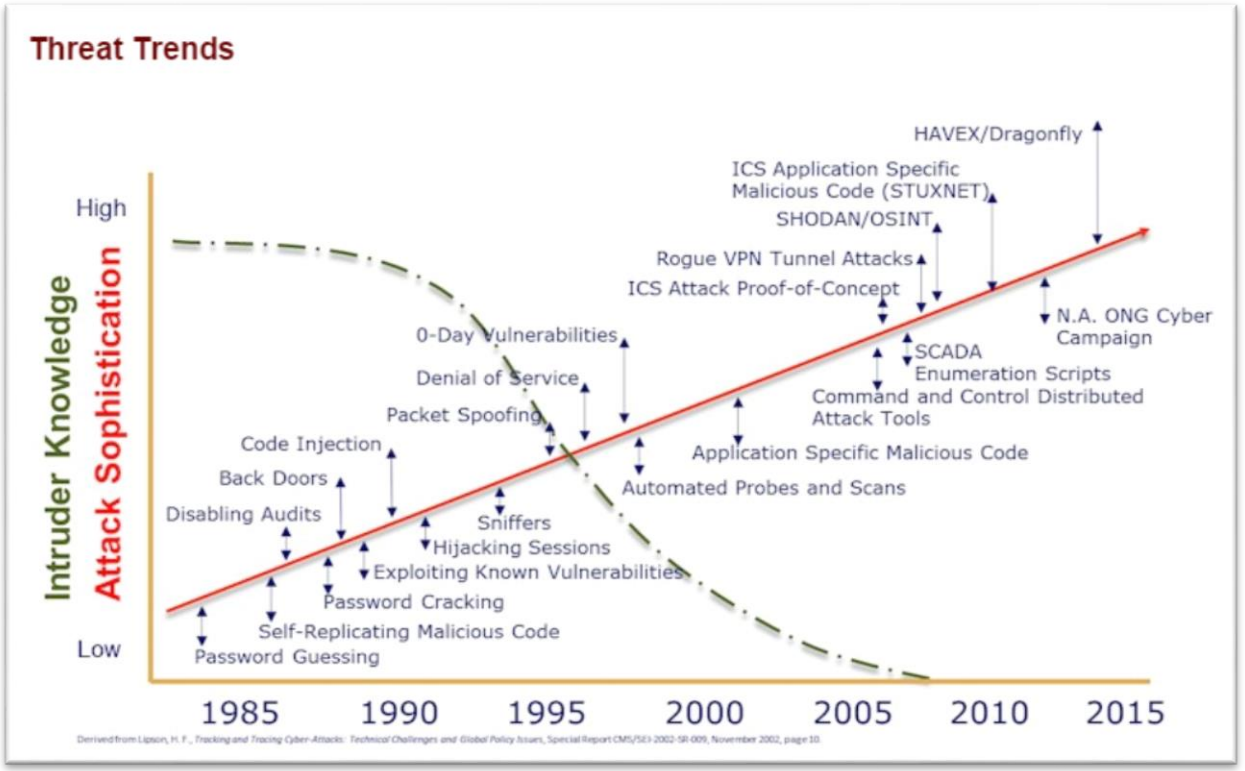
Banky (stale), CZ

Black-out (2014), Něměcko

Uživatel

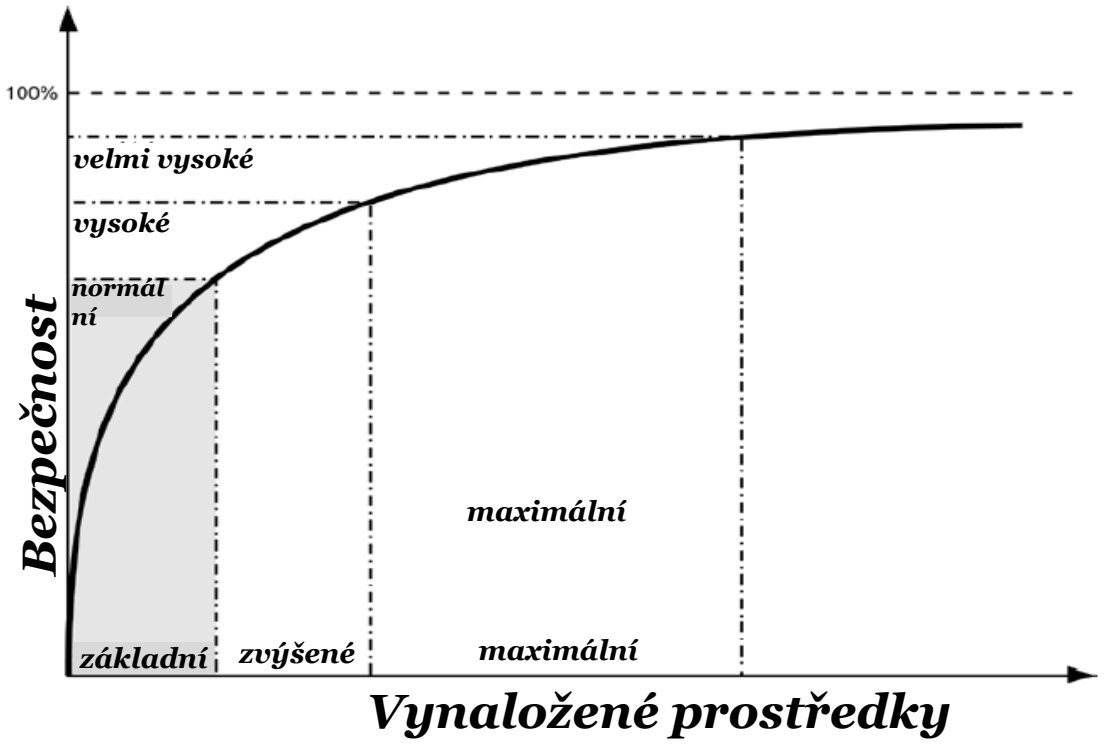
Kybernetický útok - statistika

Bude lépe? ***Nebude!***



Kybernetický útok – náklady

Kolik má smysl investovat?



Kybernetický útok – novinky

Tradiční kybernetické útoky:

- Webové stránky
- Uživatelské počítače
- Servery
- Síťová infrastruktura

Nové vektory kybernetických útoků:

- IoT
- SCADA
- Automatizace, Roboti

Kdo je útočník

Jak si ho všichni představují:

Realita bývá jiná

Kdo je útočník – kde ho najít

Lidé se dají najmout na všechno:

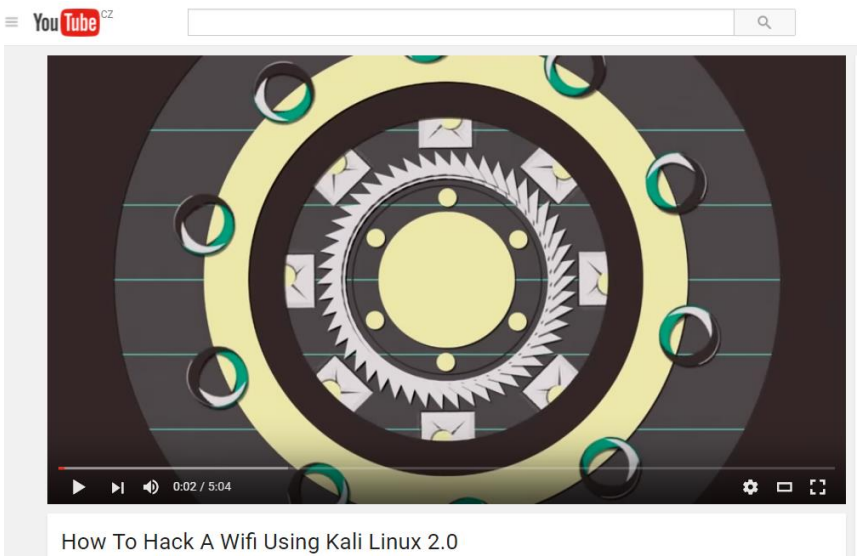
- Tor síť – šedá zóna internetu, internet v internetu.

Nástroje vhodné k útoku jsou “běžně” dostupné

- Malware
- Botnet již od:
  - $25 pro 1,000 host,
  - $110 pro 5,000 host
  - $200 pro 10,000 host.

Naučit se to

- https://www.youtube.com/watch?v=i8kxuci_XCo



Proč útočí - výdělek

"Peníze jsou jenom jedny"

- **Ransomware –** výkupné za zašifrovaná data
- **Prodej Osobních údajů**, např. čísla kreditních karet, sociálních pojistek, pasů, občanských průkazů
- Seznam zákazníků společnosti a jiná **konkurenční data**
- **Zdrojové kódy** softwaru a know-how

Proč útočí - nenávist

- **Konkurenční boj** – DoS na webové stránky
- **Deziluze ze ztráty zaměstnání** – Únik citlivých informací
- **Průmyslová špionáž** – Únik know-how, změny v datech
- **Osobní zájem** - cokoliv
- **Boj aktivistů** – boj proti globalizaci, korporacím, ropným společnostem, atd. – jakékoliv poškození je vítané

Proč útočí – státní zájem

Díky IT je možné špionáž provádět i z postele – zrychlení, zjednodušení a efektivita je obrovská.

Motivace

- Získání strategických informací
- Poškození obrany schopnosti / konkurence schopnosti

Oblasti zájmu

- Jaderný program
- Obrana
- Zásobování zdroji

Proč útočí – protože to jde

Najít návody na YT je jednoduché, proč to nezkusit…

…chci ostatním ukázat co umím.

Motivace

- Prostě to zkusit
- Pochlubit se

Oblasti zájmu

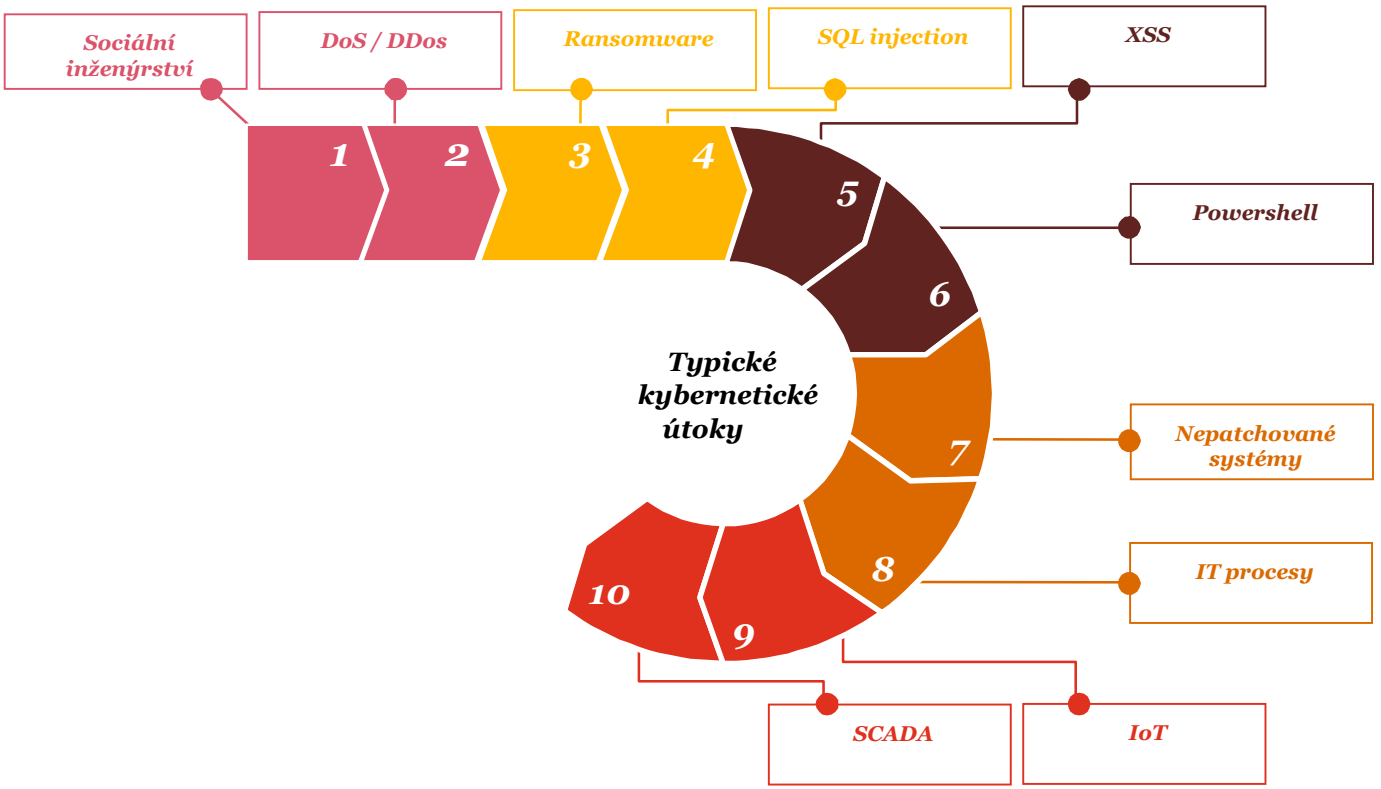
- Lokální společnosti
- Veřejně známé společnosti
- Osobnosti

Důsledky

- U amatérů lehce vystopovatelný zdroj
- Právní důsledky

Vektory útoku

Lehký úvod do nejznámějších vektorů kybernetického útoku…



Vektory útoku – Sociální inženýrství

Společnost

Prerekvizity:

- Důvěřiví zaměstnanci

Odhalení:

- Středně obtížné

Riziko:

- Kritické

Dopady:

- Kompletní ztráta kontroly
- Ztráta dat
- Nevratné změny v procesech

Útočník

Prerekvizity:

- Email, USB flash, telefon

Složitost útoku:

- Střední

Postup:

1. Získat důvěru
2. Dostat svůj kód do společnosti
3. Aktivovat hrozbu a využít vnitřních zranitelností

Vektory útoku – DoS, DDoS

Společnost

Prerekvizity:

- Zranitelné prostředí

Odhalení:

- Jednoduché

Riziko:

- Vysoké

Dopady:

- Neschopnost komunikovat
- Zahlcení všech služeb
- Konsekvence s návaznými procesy

Útočník

Prerekvizity:

- Botnet

Složitost útoku:

- Nízká

Postup:

1. Zakoupit botnet
2. Definovat adresu

Vektory útoku – Ransomware

Společnost

Prerekvizity:

- Zranitelné prostředí

Odhalení:

- Jednoduché

Riziko:

- Kritické

Dopady:

- Finanční ztráta
- Úplná ztráta dat

Útočník

Prerekvizity:

- Malware schopný kryptovat cizí data

Složitost útoku:

- Vysoká

Postup:

1. Dostat malware do vnitřního prostředí společnosti (soc.ing atd.)
2. Spustit šifrovací mechanismus
3. Oslovit “zákazníka” a nabídnout vrácení dat.

Vektory útoku – SQL injection / XSS

Společnost

Prerekvizity:

- Zranitelné prostředí

Odhalení:

- Složité

Riziko:

- Kritické

Dopady:

- Úplná ztráta dat (SQLi)
- Modifikace dat (SQLi)
- Krádež identity (XSS)

Útočník

Prerekvizity:

- Přístup k webové stránce

Složitost útoku:

- Jednoduchá

Postup:

1. Nalezení zranitelného formuláře
2. Použití SQL injection / XSS techniky (VIZ TABULE)
3. Volný pohyb po databázi / získání identity

Vektory útoku – Powershell

Společnost

Prerekvizity:

- Zranitelné prostředí

Odhalení:

- Složité

Riziko:

- Kritické

Dopady:

- Úplná ztráta dat
- Modifikace dat
- Ztráta přístupových oprávnění
- Ztráta kontroly nad prostředím

Útočník

Prerekvizity:

- Powershell script
- “webserver”

Složitost útoku:

- Složitá

Postup:

1. Spuštění powershell skriptu na napadeném PC
2. Sestavení spojení k “webserveru”
3. Stažení a sestavení kompletního agenta
4. Ovládání agenta a celého počítače přes vzdálený server

Vektory útoku – Nepatchované systémy

Společnost

Prerekvizity:

- Nepatchované systémy

Odhalení:

- Složité

Riziko:

- Kritické

Dopady:

- Destrukce infrastruktury

Útočník

Prerekvizity:

- Znalost kritických zranitelností

Složitost útoku:

- Středně složitá

Postup:

1. Odhalení nepatchovaného systému
2. Definice zranitelností verze systému
3. Zneužití těchto známých zranitelností

Vektory útoku – IT procesy

Společnost

Prerekvizity:

- Nedokonalé IT procesy

Odhalení:

- Složité

Riziko:

- Kritické

Dopady:

- Úplná ztráta dat
- Modifikace dat a procesů
- Ztráta know-how
- Neschopnost fungování společnosti

Útočník

Prerekvizity:

- Znalost procesů společnosti

Složitost útoku:

- Středně složitá

Postup:

1. Odhalení nefungujících / nesledovaných procesů
2. Zneužití interních procesů pro aktivaci jiných hrozeb nebo získání přístupu k informacím.

Vektory útoku – IoT / SCADA

Společnost

Prerekvizity:

- Organicky rostlé IoT / SCADA

Odhalení:

- Složité

Riziko:

- Kritické

Dopady:

- Neschopnost společnosti využívat IoT technologie
- Zastavení všech návazných procesů
- Hmotné i nehmotné ztráty
- Ztráty na životech

Útočník

Prerekvizity:

- Znalost IoT infrastruktury

Složitost útoku:

- Středně složitá

Postup:

1. Získání přístupu k nezabezpečené IoT / SCADA infrastruktuře
2. By-pass komunikace
3. Podvržení signálů

Vektory útoku - soutěž

Zadání:

Použijte jednu z výše popsaných technologií ke získání přístupu do zabezpečené sekce stránky **hackit.cz**

Vyhodnocení:

Na konci přednášky. Ceny pro několik prvních “hackerů”. ☺

Jak se bránit - technika

1. Risk analýza – definice toho, co je opravdu třeba chránit.
2. Penetrační testy – nezávislé, pravidelné a v dostatečném rozsahu
3. Revize FW pravidel
4. Investice do monitoringu – SIEM, IPS, IDS
5. Sledovat aktuální trendy a nejít slepě za efektivním využíváním IT

Jak se bránit - lidé

1. Sociální inženýrství – pravidelné testování připravenosti zaměstnanců
2. Školení – v dostatečném rozsahu a pravidelně
3. Motivace zaměstnanců
4. Správná správa třetích stran
5. Právní zajištění
6. Dostatečný počet správců IT, zajištění role CISO a jeho správné umístění ve struktuře

Jak se bránit - procesy

1. Řízení přístupových oprávnění
2. Pravidelný audit procesní bezpečnosti a efektivity
3. Detailní sledování administrátorů
4. Nastavení incident managementu
5. Zajištění service desku
6. Definice předpisové základny
7. Simulace kybernetického útoku na procesní úrovni

Vyhlášení vítězů

Gratulujeme!

Řešení je například:

a' or 1 --

Budoucnost kybernetické bezpečnosti

“Kybernetická bezpečnost je a bude stále důležitější součásti profesního i osobního života.”

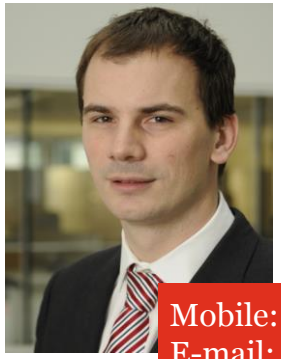
“Technologický vývoj přináší mnoho nových možností, ale také otázek bez odpovědí.”

Vaše budoucnost?

“Kvalitní profesionálové v oblasti kybernetické bezpečnosti jsou již nyní nedostatkové zboží a i v budoucnu budou placeni zlatem.”

www.pwctechnology.cz

Kontakt



Michal Čábela
Assistant manager

Mobile: +420 775 214 115
E-mail: michal.cabela@cz.pwc.com