Skutečnost může být horší než očekávání

Společnost AEC úspěšně eliminovala rozsáhlý phishingový útok na tuzemskou finanční instituci

Finanční instituce napadená mezinárodní hackerskou skupinou se pokoušela vyřešit problém vlastními silami. Nakonec však byla nucena požádat o pomoc tým expertů na kybernetickou bezpečnost. Lidé z AEC dokázali do dvou hodin od seznámení se s případem odhalit nebývalý rozsah incidentu. Útok trval několik týdnů a útočník ovládl značné množství serverů, pracovních stanic i privilegovaných účtů.

zločinecká skupina Cobalt Group **finanční instituce** **zastavení útoku**
ochrana koncových zařízení

Je konec roku 2019. Pro IT administrátora jedné z tuzemských finančních institucí jen další den běžné rutiny. Jako obvykle v tuto dobu monitoruje cvrkot na síti, ale náhle zpozorní.

„Děláš teď něco s doménou?“ obrátí se na kolegu.
„Ne.“
„Tak proč náš admin účet přistupuje k datům na půlce všech firemních serverů?“

Co může stát za nestandardní aktivitou účtu doménového administrátora Active Directory domény? Jedná se o „klíč ke království“ – tenhle účet poskytuje vlastníkovi ve většině případů „absolutní moc“, ať už přímou, či nepřímou, nad celou IT infrastrukturou. Tedy i nad daty a business aplikacemi, které instituce provozuje. Následuje několik dnů interního vyšetřování. Jako nejpravděpodobnější se zpočátku jeví zneužití přístupu třetí smluvní stranou. Ale všichni z outsourcerů, kteří spravují jeden z interních systémů společnosti, na zdvořilý dotaz okamžitě a důrazně odmítají jakoukoli práci mimo sjednaný rozsah. Takže útok? Na nás? Je to vůbec možné?

Když vlastní síly nestačí

Uvedená společnost, která nepatří na tuzemské finanční scéně ke zcela marginálním hráčům, používá pro účely bezpečnostního monitoringu nástroje SIEM (Security Incident and Event Management). Ty jsou z pohledu „log managementu“, tj. sběru a uchovávaní logů, ve výrazně lepší kondici, než je tomu v případě běžného českého průměru. Jen sbírat logy však pro detekci útoku nestačí. Některé z monitorovacích pravidel alertují nestandardní aktivity, ale tyto alerty se ztrácejí mezi množstvím jiných, méně významných upozornění.

Dobře posbírané logy v SIEM systému mohou posloužit k manuálnímu vyšetření incidentu. Oddělení bezpečnosti dané instituce tento systém využívá a nachází podezřelé aktivity v auditních záznamech Active Directory pro jeden účet na serveru, na kterém pracovala třetí strana.

I když společnost není schopná identifikovat vstupní vektor útoku ani jeho rozsah či způsob vzdálené komunikace útočníka, padne rozhodnutí čelit protivníkovi vlastními silami. Pracovníci IT oddělení firmy začínají postupně měnit hesla k vybraným privilegovaným účtům, dočasně vypínají dotčený server a zahajují masivní záplatování zranitelností. Intenzita nestandardních aktivit privilegovaných účtů v prostředí však i přes všechna tato opatření roste. Management finanční instituce je konfrontován se stávající situací a na doporučení rozhoduje bez prodlení

oslovit společnost AEC, která se specializuje na poskytování služeb v oblasti kybernetické bezpečnosti.

A na počátku byl phishing

Přestože uvedená finanční instituce nebyla klientem AEC a bezpečnostní firma nedisponuje nadbytečnými kapacitami, uvolní dočasně několik analytiků svého Cyber Defense Centra. Prvotní seznámení se se situací a s podezřeními na probíhající útok trvá expertům centra zhruba hodinu. Dosavadní opatření proti útoku jsou shledána jako zcela nedostatečná – reset hesel vybraných účtů zkušeného útočníka nemůže zastavit. Rovněž dosud nebyly identifikovány persistenční mechanismy (zadní vrátka), které útočník do prostředí během své déletrvající aktivity umístil.

Vzhledem k tomu, že není jasné ani to, zda útočník aktivně exploatoval (zneužil) zranitelnosti, nemusí být pro danou situaci relevantní ani jejich záplatování. Lidé z AEC přistupují k detailnímu náhledu do SIEM systému. K ověření probíhajícího útoku a k odhalení většiny klíčových podrobností potřebují další dvě hodiny. Zjištění se v mnohém výrazně liší od původních odhadů finanční instituce:

1. Útok začal v tichosti o několik týdnů dříve, než jej instituce zaregistrovala.
2. Útok začal kompromitací pracovní stanice jednoho z uživatelů businessu, nikoli serveru spravovaného třetí stranou. Tento uživatel totiž otevřel phishingový e-mail.
3. Útočník ovládl v prostředí značné množství serverů a pracovních stanic, nikoli jen jeden server.
4. Útočník ovládl v prostředí mnoho účtů (včetně privilegovaných), nikoli jen domnělé účty, u kterých proběhly změny hesel.
5. Mnohé z infikovaných serverů a stanic aktivně komunikují do internetu na CnC (Command and Control). Jedná se o infrastrukturu, která je dle zdrojů používaná skupinou Cobalt Group.

[1] https://www.itp.net/617212-billion-euro-cybercrime-group-strikes-again

Za vším hledej peníze

Hackerská skupina Cobalt Group je známá svými aktivitami po celém světě. Nejčastěji však útočí na finanční instituce ve východní Evropě a Asii. Její sofistikované útoky jsou finančně motivované, specializují se na vyvedení finančních prostředků prostřednictvím napadení ATM (bankomatových) systémů a systému SWIFT. Dle některých odhadů[1] se skupině podařilo tímto způsobem dosud ukrást řádově až 1 mld. $. Používá ke svým útokům mimo jiné i běžně dostupné prostředky, jako např. útočný framework Cobalt Strike, zneužití PowerShell nebo Mimikatz pro extraci hesel (či hashů hesel) v prostředí Windows.

Veškeré tyto nástroje detekovali experti AEC i během stávajícího útoku. Jejich podezření ukazující správným směrem potvrzovala i komunikace s CnC infrastrukturou (DNS doménami a IP adresami) přisuzovaná právě hackerské skupině Cobalt Group. Poté, co se definitivně potvrdilo, že se instituce nachází pod aktivním APT (Advanced Persistent Threat) útokem finančně motivovaného a velmi zkušeného útočníka, byly společně stanoveny tři primární cíle:

1. zastavení útoku,
2. identifikace vstupního vektoru,
3. analýza rozsahu kompromitovaných dat a systémů.

Zastavení útoku

Vraťme se na začátek. Instituce zaregistrovala nestandardní chování ve svém systému. Po nějaké době jej vyhodnotila jako pokus o útok a následně se pokoušela útočníka zastavit vlastními kapacitami. Protože odpovědní pracovníci společnosti neměli v té době představu o celkovém rozsahu útoku, nemohla být jejich snaha o vyřešení incidentu úspěšná.

Útočník velmi záhy jejich nesystematické pokusy zaznamenal a obratem začal používat jiné privilegované účty, pohotově vytvořil nové persistenční mechanismy (viz Obr. 1) a také jinou CnC infrastrukturu na internetu.

Poté už ale převzal taktovku tým z AEC. Základem úspěšného zastavení útoku bylo současné a koordinované provedení několika kroků. Zaprvé byla opakovaně změněna hesla všech (nikoli jen privilegovaných) účtů v Active Directory doméně. Zadruhé byly vypnuty koncové stanice a servery s prokazatelnou komunikací na CnC infrastrukturu útočníka. Zatřetí byly zásadním způsobem upraveny politiky přístupu na internet na webové proxy. Bod čtyři je nejdůležitější – byl nasazen nástroj EPP/EDR (Endpoint Protection Platform/Endpoint Detection and Response), který části útoku zastavil automaticky a části útoku detekoval pro manuální ukončení týmem AEC.

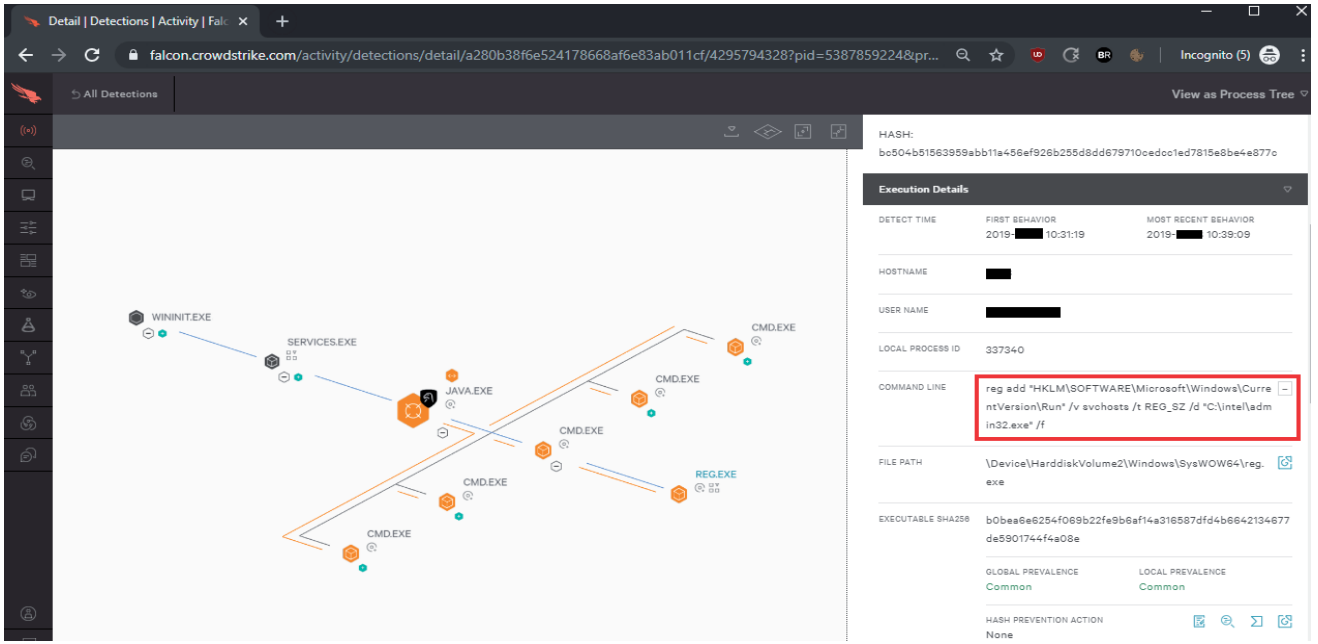
V ideálním případě je při nasazení EPP/EDR proveden restart serveru či koncové stanice. Po restartu má EPP/EDR agent možnost sledovat útočné aktivity při jejich startu, a díky tomu disponuje klíčovou výhodou v podobě výrazně zvýšené schopnosti jejich detekce. Hromadný restart serverů ale neproběhl, proto byly některé persistentní mechanismy, které útočník do prostředí umístil, aktivovány poměrně záhy. Jednalo se o automatický start škodlivého programu po přihlášení konkrétního IT zaměstnance na konkrétním počítači nebo o automatický start při startu serveru.

V době, kdy bylo EPP/EDR řešení nasazeno teprve pár dnů, nebyla jeho schopnost prevence ještě nastavena na stupeň agresivní. Některé kroky útočníka tak dosud nemohly být automaticky zablokované. V rámci agresivní detekce proto bylo nutné útočníka zastavit manuálně. Právě tato fáze byla pro specialisty, kteří se zabývají kybernetickou ochranou, mimořádně zajímavá. Umožnila jim studovat takřka v přímém přenosu kroky a chování útočníka, který si již musel být vědom toho, že se blíží konec jeho „dobrodružství" v prostředí napadené instituce.

Jedním z prvních kroků se útočník pokusil spustit nástroj Mimikatz (pro extrakci hesel a hashů hesel) k jiným účtům. Tento nástroj je natolik známý, že byl zablokován automaticky. Tato aktivita částečně potvrdila účinnost změny všech hesel, protože útočník se usilovně, ale neúspěšně snažil získat přístup k heslům novým. Následně se pokusil vytvořit další zadní vrátka na jednom ze serverů, konkrétně vytvořil nový privilegovaný účet (viz Obr. 2). Je pravděpodobné, že v této fázi byl už pod značným tlakem, protože spěchal a udělal mnoho překlepů.

Velmi zajímavé byly rovněž útočníkovy pokusy odinstalovat EPP/EDR nástroj (viz Obr. 3), což se mu nakonec kvůli neznalosti odinstalačního tokenu nepovedlo. I tyto poslední „záchvěvy" byly zastaveny a zbývající aktivní přístupy útočníka do systému ukončeny.

Po několika týdnech minimálních zásahů do konfigurace (zejména kvůli oprávněně podezřelým aplikacím využívaných IT týmem), byla i prevence nastavena do agresivního režimu. Útok APT probíhající po dobu mnoha týdnů zastavil tým specialistů z AEC během několika dnů. Kompletně eliminována byla činnost útočníka v systému napadené finanční instituce do dvou týdnů od okamžiku, kdy se tým AEC vložil do hry.



Obr. 1: Útočník vytvářející persistenci pomocí jednorázové a vzdálené služby java.exe: automatický start malwaru admin32.exe pomocí klíče v registrech `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` *maskující se za standardní process svchost*

Identifikace vstupního vektoru

Útok byl zastaven, útočník eliminován. Ale co když se pokusí do téhož prostředí vrátit? Je třeba mít naprosto přesnou představu o tom, jak se do systému dostal. Při detailní analýze byly identifikované phishingové e-maily doručené do e-mailových schránek několika zaměstnanců (viz Obr. 5).

Odesílatelem byla věrohodná (a nepodvržená) e-mailová adresa českého telekomunikačního operátora. Adresátem e-mailů pak bylo vždy několik zaměstnanců (současných, ale i bývalých) většiny finančních institucí v České republice. Úspěšně napadená instituce tedy nebyla

```
net  localgroup Administraotrs guest /add
net  user Guest fXXXXXXX1
net  user Guest /active:yes
net  user Guest
net  localgroup GUests guest /del
net  localgroup GUests guestt /del
net  localgroup Administrators guest /add
```

Obr. 2: Jedny z posledních aktivit útočníka v prostředí. Pokouší se vytvořit zadní vrátka pomocí účtu Guest, který aktivuje a poskytuje práva administrátora. Má naspěch a dělá chyby (viz překlepy).

jediným výlučným cílem útočníka, což je vždy dobrá zpráva. Útočníkovi šlo o peníze, ne o konkrétní instituci, a pravděpodobnost jeho návratu je tedy nižší.

Odesílatel zprávy žádal příjemce lámanou češtinou o zaplacení faktury připojené údajně v příloze. Text byl zjevně strojově překládán z cizího jazyka, přičemž některé jeho části (např. 18.10.2019r) naznačují, ze kterého. Součástí e-mailu byla i excelová příloha. Po jejím otevření se však žádná avizovaná faktura neobjevila. Naopak se spustil škodlivý Visual Basic script, který začal okamžitě komunikovat na CnC server útočníka na internetu. Obr. 4 ukazuje, jak taková komunikace vypadá v případě, kdy ji webová proxy blokuje, a v případě, kdy ji neblokuje.

Postupně se ukázalo, že několik zaměstnanců instituce přílohu otevřelo, zachránila je však webová proxy. Ale u jednoho z uživatelů byla aplikována výjimka v nastavení proxy a komunikace na CnC server na internetu byla povolena. Poté, co útočník rozeslal stovky phishingových e-mailů, mu tato jediná skulinka umožnila vkročit do prostředí. Jeho následné kroky zanechaly množství stop: nestandardní komunikace do podezřelých států, blokace některých kroků antivirem nebo přihlášení na vysoce privilegovaný účet Active Directory. To vše během pár desítek minut od úvodní infekce. Některé z těchto stop byly dostupné v bezpečnostním monitoringu SIEM, ale v závalu dalších alertů zůstaly nepovšimnuty.

Jedním z protiopatření zabraňujících útočníkovi použít uvedený vektor k opakovanému vstupu do prostředí je zmiňovaný nástroj EPP/EDR. Jeho účinnost byla ověřena i při masivních phishingových kampaních na české finanční instituce v prosinci 2019. Navzdory intenzivní osvětě se mezi zaměstnanci zde pojednávané finanční instituce objevují i nadále tací, kteří otevírají škodlivé přílohy podvržených e-mailů. Veškeré tyto pokusy jsou však naštěstí včas zablokovány EPP/EDR řešením bez postranních false positive hlášení.

- File Name: \Device\HarddiskVolume2\ProgramData\Package Cache\{0d38521f-fdee-4bf0-a283-e8f74b153fe8}\WindowsSensor.x64.exe
- CommandLine: "C:\ProgramData\Package Cache\{0d38521f-fdee-4bf0-a283-e8f74b153fe8}\WindowsSensor.x64.exe" -burn.clean.room="C:\ProgramData\Package Cache\{0d38521f-fdee-4bf0-a283-e8f74b153fe8}**WindowsSensor.x64.exe**" -burn.filehandle.attached=328 -burn.filehandle.self=336 **/uninstall**
- SHA256: d81da6de19f0dd5bcdcaeffb760facbb2186138aa1988806292dd45ccf2ee681
- MD5: 4584c277cc9331d9097c199f2dddfa5e
- PID: 5972
- Parent ProcessId: 110552480858

Obr. 3: Útočník zaregistroval běžícího EPP/EDR agenta a neúspěšně se ho snaží odinstalovat

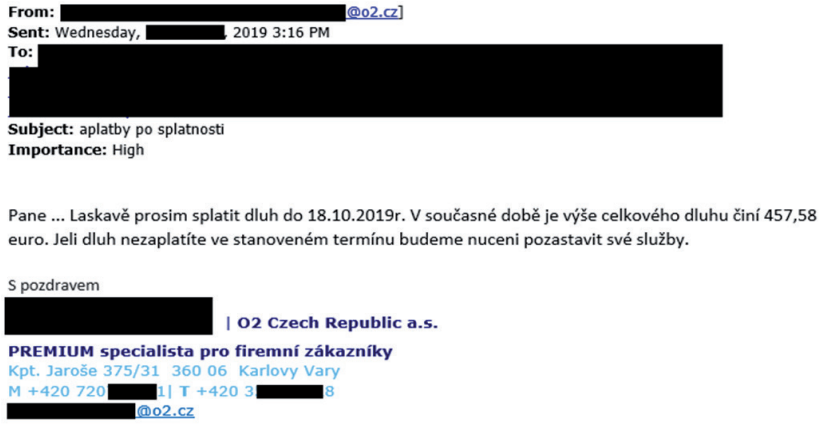
```
<30>XXX XX XX:18:16 XXX-XX mwg: LEEF:1.0|XXXXXX|Web
Gateway|7.8.2.11.0|22|devTime=15XX022296000|src=XXX.XX.X.133|usrName=XXXXXXXX|httpStatus=403|
dst=XX.XX.12.4|urlCategories=Business|blockReason=Media type
blocked|url=https://www.octetfruitsllc.com/vendor/phpunit/phpunit/src/Util/PHP/avatar.hlpv

<30>XXX XX XX:18:30 XXX-XX mwg: LEEF:1.0| XXXXXX |Web
Gateway|7.8.2.11.0|0|devTime=15XX022310000|src=XXX.XX.X.27|usrName=|httpStatus=200|dst
=X.X.X.X|urlCategories=|blockReason=|url=https://www.octetfruitsllc.com

<30>XXX XX XX:20:36 XXX-XX mwg: LEEF:1.0| XXXXXX |Web
Gateway|7.8.2.11.0|0|devTime=15XX022436000|src=XXX.XX.X.27|usrName=|httpStatus=200|dst
=X.X.X.X|urlCategories=|blockReason=|url=https://0345432456.info
```

Obr. 4: Pro většinu uživatelů, kteří otevřeli phishingovou přílohu, je komunikace s CnC infrastrukturou zablokovaná. Jeden uživatel má ale nezdokumentovanou výjimku, takže jeho PC může neautentizovaně komunikovat s proxy a proxy nedešifruje HTTPS komunikaci.

Bez ohledu na přetrvávající potíže týkající se přístupu některých zaměstnanců k podezřelým e-mailům lze ve věci identifikace vstupního vektoru do prostředí napadené instituce konstatovat, že tým AEC expertů kompletně identifikoval průběh útoku a detailně popsal přesný způsob vniknutí do systému a rozsah aktivit, které v něm útočník prováděl.


From: [redacted]@o2.cz]
Sent: Wednesday, [redacted], 2019 3:16 PM
To: [redacted]
Subject: aplatby po splatnosti
Importance: High

Pane ... Laskavě prosim splatit dluh do 18.10.2019r. V současné době je výše celkového dluhu činí 457,58 euro. Jeli dluh nezaplatíte ve stanoveném termínu budeme nuceni pozastavit své služby.

S pozdravem
[redacted] | O2 Czech Republic a.s.
PREMIUM specialista pro firemní zákazníky
Kpt. Jaroše 375/31 360 06 Karlovy Vary
M +420 720 [redacted]1| T +420 3[redacted]8
[redacted]@o2.cz

Obr. 5: Phishingový e-mail, který obdrželi zaměstnanci finanční instituce

Analýza rozsahu kompromitovaných dat

Jednou z důležitých otázek bylo, jaká data byla kompromitována. Mohlo se jednat o neoprávněnou modifikaci (tj. narušení integrity) nebo o neoprávněný náhled (tj. narušení důvěrnosti). Jakkoli je tato otázka zajímavá a důležitá, není na ni možné ani s odstupem podat jednoznačnou a důkazy podloženou odpověď. Mezi úvodní kompromitací prostředí a zastavením útoku uběhly řádově týdny. Útočník přistoupil k mnohým interním systémům, např. e-mailovým systémům a sdíleným složkám s pracovními dokumenty některých oddělení společnosti. Pro pohyb v prostředí využíval standardních služeb Microsoft prostředí, např. administrátorské shary IPC$, vzdálené plánování služeb nebo obfuskované Powershell skripty. Útočník využíval privilegované účty, které byly (oproti best-practice) používané pro rutinní práci IT týmu a některých IT systémů. Odlišení aktivit útočníka od standardního chodu IT proto bylo složité, někdy dokonce zcela nemožné.

Na otázku, jaká data byla kompromitována, můžeme odpovědět následovně: z auditních stop dostupných v rámci vyšetřování nebyly nalezeny důkazy o narušení integrity dat v databázích a aplikacích. Rovněž nebyly nalezeny důkazy o extrakci dat z důvěrných systémů mimo instituci.

Jak problémům předcházet aneb zašněrujte si tkaničky u bot

Ochrana koncových stanic je často opomíjená, protože při analýzách rizik toto aktivum buď zcela chybí, nebo jsou jeho business dopady (a potažmo související rizika) hodnocené jako nízké. Jsou to ale právě koncová zařízení, která mnohdy útočníkovi umožní prvotní vstup do prostředí, např. formou phishingu.

Nelze se spoléhat na to, že bezpečnostní opatření budou plně funkční vždy a za každých okolností.

- Mnoho phishingových e-mailů bylo zastaveno na vstupní e-mailové bráně, ale ne všechny.
- Většina zaměstnanců v tematizovaném případě e-mail neotevřela, ale našli se tací, kteří ano.
- Většina úvodních pokusů o komunikaci s CnC serverem byla zablokovaná, pro jednoho uživatele však nikoli.
- Některé pokusy ze strany útočníka byly zablokovány lokálním antivirem, ale ne všechny.
- Bezpečnostní dohledový systém SIEM některé části útoku detekoval v reálném čase, ale tyto důležité alerty zanikly v běžném provozním šumu.

IT hygiena při využívání privilegovaných účtů je důležitá nejen pro provoz, ale také pro bezpečnost. Práce s těmito účty (administrátorské, servisní, aplikační atd.) by měla mít jasná pravidla s nastavenou kontrolou jejich dodržování. Předešlo by se tak problémům při investigaci, kdy byl v jednom čase na stejném serveru využíván tentýž účet jak útočníkem, tak interním IT zaměstnancem (nejednalo se samozřejmě o tu samou personu).

Při segmentaci sítě je vhodné rozlišovat nejen servery od koncových zařízení, ale také jednotlivé aplikace, prostředí (produkční, testovací, vývojové), organizační strukturu (IT a non-IT) atd. Útočník měl v tomto případě příliš jednoduchou cestu – mohl se vydat libovolným směrem, kterým se mu zachtělo. Ale možná to úplně nejdůležitější doporučení se týká kontinuálního vzdělávání zaměstnanců. Ti by měli být mimo jiné schopni odlišit podvržený e-mail, neotevírat ho, resp. nebát se ohlásit otevření podezřelé přílohy bezpečnostnímu týmu.

Závěrem je třeba konstatovat jeden nezpochybnitelný fakt. Pro běžnou firmu či instituci bez ohledu na její velikost či obor zájmu je velmi obtížné odolat motivovanému útočníkovi, který má pro financování svých aktivit k dispozici ukradenou miliardu dolarů.

Ale i přes veškeré komplikace, nejasnosti a nástrahy nakonec pro každou společnost existuje jeden úplně poslední a poněkud drsný důvod, proč se řídit poznatky vyplývajícími z našeho textu a ostatními best-practise doporučeními. Pojednává o tom moc hezký příběh. Dva poutníci jdou po poušti, když tu spatří, jak se k nim z dáli řítí hladový lev. Jeden z nich se bleskurychle sehne a začne si co nejpevněji utahovat tkaničky u bot. *„Myslíš, že ti pomůže utéct mu?“* ptá se ho ten druhý. *„Asi ne. Ale mně stačí, když budu rychlejší než ty.“*

Martin Hlaváč
???@???

Martin Hlaváč

Pracuje v oblasti informační bezpečnosti od roku 2006. Věnoval se celému spektru témat počínaje tvorbou bezpečnostních politik a standardů přes zabezpečení integrity kritických finančních toků až po bezpečnostní monitoring a reakci na incidenty. V posledních letech se zaměřuje především na návrh, implementaci a provoz služeb souvisejících se SOC (Security Operations Center) a IR (Incident Response). V současné době působí jako technický garant služeb CDC (Cyber Defense Center) ve společnosti AEC a.s.