

Vytvoření Security Operation Centra

Motivace a úskalí

20. 4. 2016 – Konference C-level Security Day, Praha

Ing. Richard Michálek, Cybersecurity and Business Continuity expert

Security Operation Center (SOC)



Security Operation Center (SOC)

Operační středisko bezpečnosti

Operační středisko kybernetického boje

Co tvoří SOC ?

- Velké obrazovky 😊

Security Operation Center (SOC)

Operační středisko bezpečnosti

Operační středisko kybernetického boje

Co tvoří SOC ?

- **Techologie** 😊
 - obranná/útočná,
 - bezpečnostní monitoring, SIEM, IDS/IPS, AntiDDoS, ...
- **Tým**
 - dedikovaný/sdílený,
 - dovednosti a znalosti, pravidelný trénink, motivace ...
- **Procesy**
 - opravdový incident management je v tom, že se skutečně něco dělá - ne jen že existuje
 - dokumentované postupy, odpovědnosti a pravomoce

Security Operation Center (SOC)

Operační středisko bezpečnosti

Operační středisko kybernetického boje

Co tvoří SOC ?

- **Technologie**

- obranná/útočná,
- bezpečnostní monitoring, SIEM, IDS/IPS, AntiDDoS, ...

- **Tým**

- dedikovaný/sdílený,
- dovednosti a znalosti, pravidelný trénink, motivace ...

- **Procesy**

- opravdový incident management je v tom, že se skutečně něco dělá - ne jen že existuje
- dokumentované postupy, odpovědnosti a pravomoce

Security Operation Center (SOC)

Operační středisko bezpečnosti

Operační středisko kybernetického boje

Co tvoří SOC ?

- **Procesy**

- opravdový incident management je v tom, že se skutečně něco dělá - ne jen že existuje
- dokumentované postupy, odpovědnosti a pravomoce

- **Tým**

- dedikovaný/sdílený,
- dovednosti a znalosti, pravidelný trénink, motivace ...

- **Technologie**

- obranná/útočná,
- bezpečnostní monitoring, SIEM, IDS/IPS, AntiDDoS, ...

Security Operation Center (SOC)

Operační středisko bezpečnosti

Operační středisko kybernetického boje

Co tvoří SOC ?

- **Procesy**

- řekneme si co vlastně chceme aby náš SOC dělat
- zjistíme procesní vazby a výhody (úzká spolupráce s provozem ICT, spolupráce s NCKB, s PČR, další společnosti a organizace, ...)
- definicí co bude SOC zachraňovat zjistíme i jeho důležitost a význam pro organizaci (adekvátní přidělení lidských zdrojů a rozpočtu)

- **Tým**

- kolik lidí na SOC budeme potřebovat a jak velkou jejich kapacitou budeme alokovat
- prostředí a organizační zařazení (malá společnost, velká organizace, nadnárodní korporace)
- definice vlastností, zkušeností a odbornosti členů týmu (rozhodnost, stresová odolnost, nácviky situací, síťový, systémový, ...
..., aplikační, komunikační a taktický expert)

- **Technologie**

- vybraná členy SOC týmu na základě procesní definice toho co od SOCu chceme aby dělal
- při výběru je nutné zohlednit prostředí organizace, poznatky z provozu IT, zkušenosti a znalosti týmu
- před výběrem jednotlivých technologií je dobré si stanovit koncepci obrany a budování infrastruktury

Security Operation Center (SOC)

Motivace

Proč budovat a provozovat SOC v organizaci,
... a co z toho bude mít ?

Proč vytvářet a provozovat SOC

A historical look at security incidents by attack type, time and impact, 2011 to 2013

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

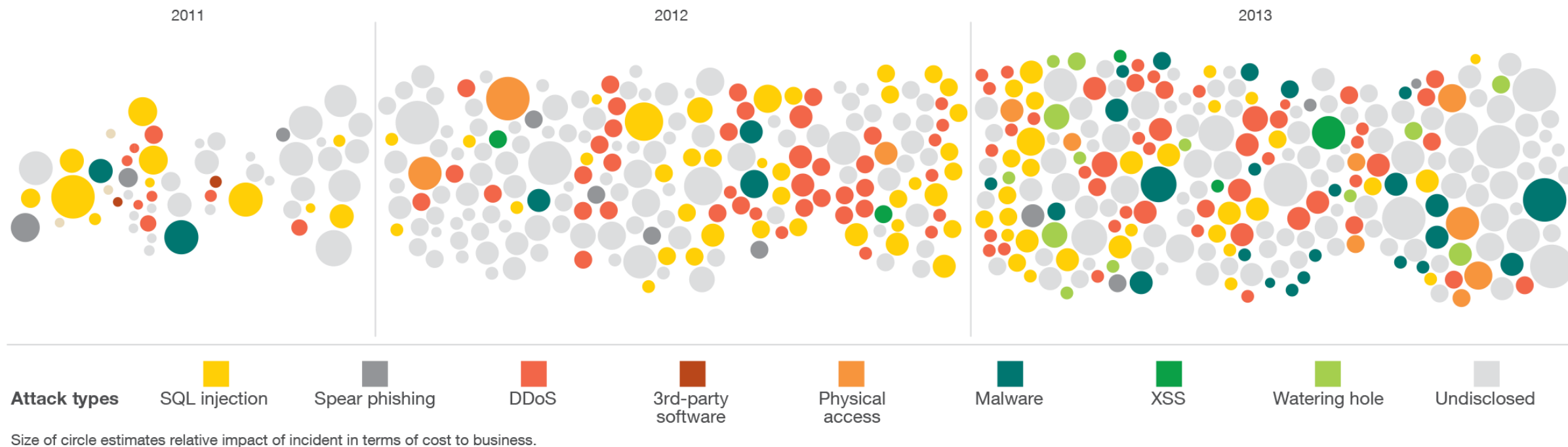


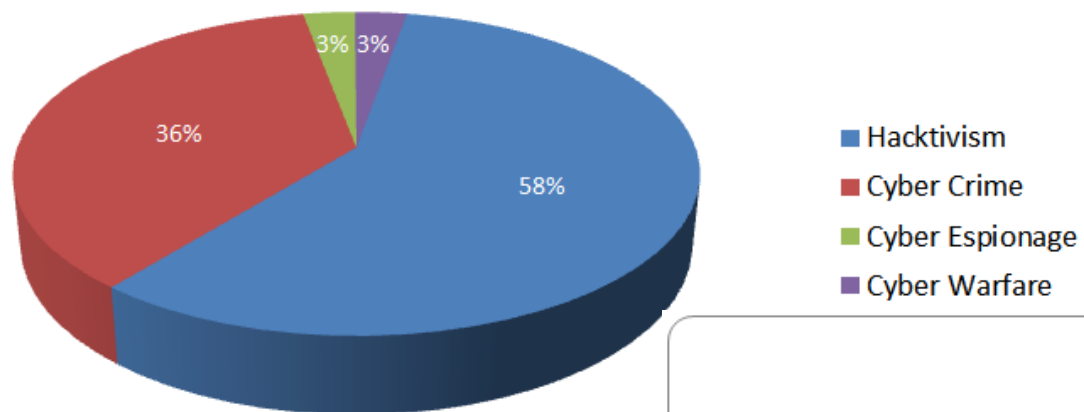
Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Source: IBM X-Force® Research and Development

Proč vytvářet a provozovat SOC

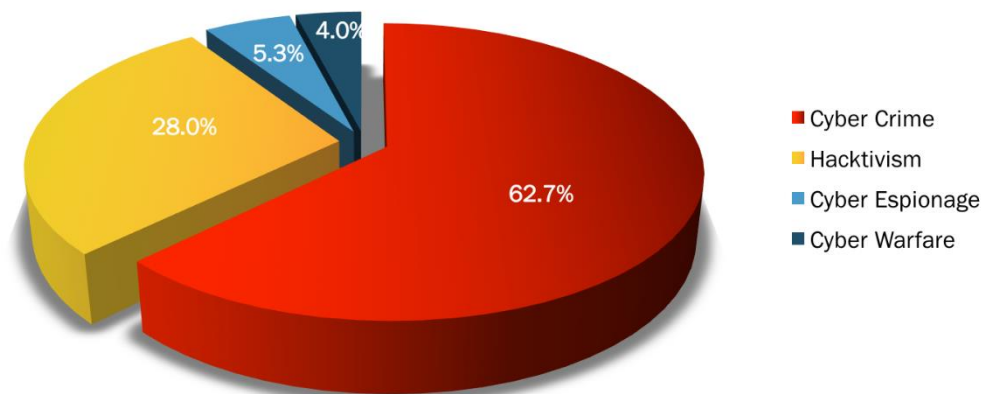
Motivations Behind Attacks

August 2012



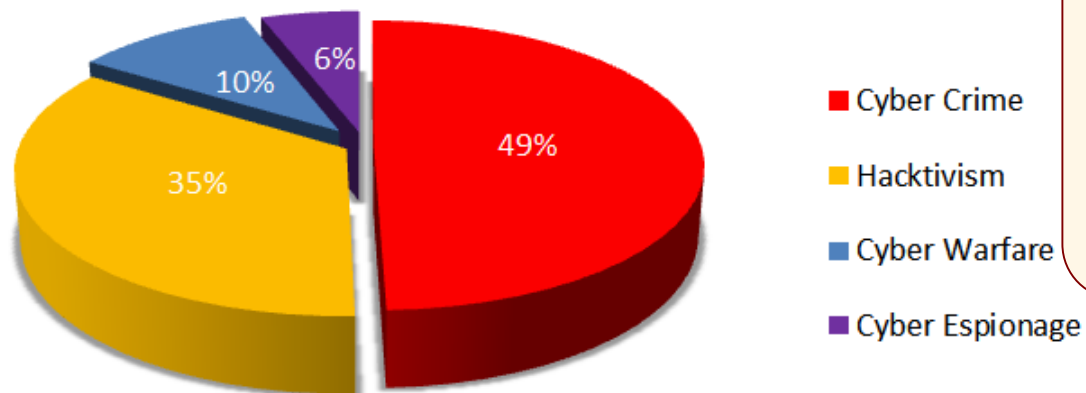
Motivations Behind Attacks

February 2016



Motivations Behind Attacks

August 2013



Motivace útočníků se mění !

2012 Cybercrime – 36%

2013 Cybercrime – 49%

2016 Cybercrime – 62%

zdroj: Hackmageddon
<http://hackmageddon.com/>

Proč vytvářet a provozovat SOC

Pohled na kyberprostor bez růžových brýlí

[Kaspersky cyber threat real-time map](https://cybermap.kaspersky.com/)

zdroj: Kaspersky Lab
<https://cybermap.kaspersky.com/>

Proč vytvářet a provozovat SOC

Organizace má právo na ochranu svých aktiv

- Hmotný majetek
- Lidé
- Informace
- Procesy
- Dobré jméno
- Svoji existenci a podnikání

Kybernetické útoky způsobují negativní dopady

- Nedostupné systémy nebo data – překážky na straně zaměstnavatele
- Škodlivý kód – botnet – zombie – přímé škody – sankce ze zákona
- DoS, DDoS – ničení obchodu a dodávky služeb – porušení smluv – výpalné
- Sniffing – odposlechnutí informací – strategická rozhodnutí – sankce
- Pozměnění údajů – škody ve vyúčtování – dobré jméno organizace
- APT – jasný cíl a dobrá taktika – vydírání zaměstnanců – získání informací
- Kyberválka – útok na slabiny (systémy, služby, lidé, politika, dobré jméno, porušení zákona, ...) – zničení společnosti či organizace

Proč vytvářet a provozovat SOC

Organizace potřebuje ochranu

- **Vnitřní nepřítel**

- Zaměstnanci
- Externisti

- **Vnější nepřítel**

- Hackeři pro radost a uznání
- Haktivisté
- Politické vlivy
- Konkurence
- Zloději
- Vyděrači
- Válečníci

Vyžaduje to zákon
181/2014Sb. o kybernetické bezpečnosti.

Už nás ty útoky stály
hodně peněz.

Někdo se o ty průšvihy
musí postarat.

Security Operation Center (SOC)

Úskalí

Co by při budování SOCu mělo být,
... a mnohdy chybí.

SOC co by mělo být a chybí

SOC v realitě šedých všedních dnů

- **SOC není vnímán jako „Operační středisko pro vedení kybernetického boje“**
 - Někdy je vnímán jako Operační středisko bezpečnosti
 - Většinou je vnímán jako pěkná a drahá hračka IT provozu nebo bezpečnosti
- **Ve válce a při ohrožení nastupují jiná pravidla**
 - Chybí „Emergency budget“ – předschválený s možností okamžitě čerpat
 - Možnost s plnou odpovědností manažera SOC vypnout část nebo celou firemní síť včetně služeb pro zákazníky (při kyberútoku rozhodují minuty)
- **Dotažení bezpečnostního incidentu k jasným výsledkům**
 - Většinou řešení incidentu končí v době jeho uhašení
 - Někdy se realizují follow-up aktivity
 - Málokdy je provedeno vyhodnocení incidentu, záznam o něm a výpočet vzniklých ztrát
 - Zprávy o incidentu jsou převážně technické a postrádají shrnutí pro vedení, ze kterého by bylo jasné co se vlastně stalo (jaký průšvih pro organizaci / business se přihodil) a co bylo díky zásahu SOC zachráněno
- **Dostatečná alokace času pro práci týmu**
 - Převážná většina SOC týmů je postavena na sdílených kapacitách řadových pracovníků s jinými úkoly
 - Není jasně definovaná priorita členů týmu ve smyslu: „V případě incidentu všeho nech a dokud nebudou dokončeny všechny fáze incidentu, nic jiného nedělej.“

SOC co by mělo být a chybí

SOC v realitě šedých všedních dnů

- **Chybí strategie a taktika kybernetického boje**

- Mnoho organizací používá strategii: „Něco uděláme a uvidíme co bude dál“ – to není špatné ... nedělat nic je horší.
– za určitých předpokladů může být i dobře funkční.

Jak definovat strategii a taktiku kybernetického boje

- **Krok 1: Poznej sebe**

- Rozpoznejte co je pro vaši organizaci skutečně důležité
- Poznejte schopnosti vašeho týmu a technologií

- **Krok 2: Poznej nepřítele**

- Sledujte trendy a vývoj praktik útočníků
- Sledujte vývoj hardwaru a útočných nástrojů

- **Krok 3: Poznej své bitevní pole**

- Informace z vulnerability management systému
- Rozpoznejte a uvědomte si své silné stránky a své slabiny

- **Krok 4: Zkontrolujte svoji schopnost alokovat zdroje**

- Finanční a lidské zdroje
- Externí zdroje a možnosti spolupráce s dalšími týmy

Strategie a taktika:

- **Strategie** – čeho chci dosáhnout
(z řeckého strategos, generál, vést)
- **Taktika** – jak toho chci dosáhnout
(z řeckého taktiké techné, umění seřadit vojsko)
- **Operativa** – je to co musím dělat abych toho dosáhnul
(pohotový, iniciativní, pružně fungující)

SOC dilemata

Nejčastější dilemata při budování – provozování SOC

- **Vlastní SOC nebo Externí služba**
 - Někdo cizí kouká na vaše problémy a potíže / třetí strana bývá nezaujatá
 - Náklady na lidi a jejich neustálý trénink / cena služeb SOC
- **Ustanovit novou organizační jednotku nebo definovat virtuální SOC tým**
 - Přesně a na 100% alokovaní odborníci / v průběhu zvládnutí incidentu lze dynamicky počet lidí navýšit o patřičné role
- **Podřídít SOC přímo generálnímu řediteli nebo ICT řediteli nebo řediteli bezpečnosti**
 - SOC by měl být nezávislý tzn. řízen někým mimo provoz ICT
 - GŘ nemusí mít vždy dostatek času, který může SOCu věnovat
 - Ideální je SOC tým v podřízenosti někoho G-1 až G-2 s možností přímého reportování GŘ

Budujeme Security Operation Center (SOC)

Před budováním SOC je dobré zvážit:

- **Operační prostředí SOCu**
 - Procesní a organizační prostředí organizace
 - Systémové prostředí ICT
- **Legislativní možnosti boje**
 - Vnitřní nepřítel
 - Vnější nepřítel
- **Legislativní a morální možnosti bezpečnostního monitoringu**
 - Uživatelé
 - Data (citlivé informace)
- **Vedení a řídicí struktury**
 - Podřízenost a pravomoce SOC (možnost zasáhnout do IT provozu)
 - Krizové řízení (zda je zavedeno/křížení pravomocí)
 - Nouzové postupy a mimořádné pravomoce (objednávka bez schválení)
- **Vhodnou strategii a koncepci obrany**
 - Pasivní/aktivní, defenzivní/ofenzivní , strategie SOC a řízení kybernetických bezpečnostních incidentů
 - Taktika kybernetického boje rozpracovaná v postupech pro zvládání incidentů

Měli bychom rovněž zhodnotit na co je společnost či organizace zralá.

Budujeme Security Operation Center (SOC)

Security Operation Center

je mnohem více, než jen technologie použité k detekci kybernetických bezpečnostních událostí.

Dobrý SOC jsou **technologie** – **procesy** – **lidé** propojené do jednoho organického celku schopného reagovat i ve výjimečných situacích.

... a právě to je to, co společnost nebo organizace potřebuje k přežití v kybernetické válce.

Vytvoření Security Operation Centra

motivace a úskalí

Děkuji za pozornost

richard.michalek@email.cz