



GDPR a kybernetická bezpečnost

Petr Zahálka Techdata

Bezpečnost je komplexní disciplína

- Ochranu objektu
 - Přístup
 - Kamerové systémy
 - Požární opatření
- Ochranu osob
- Ochranu dat
 - To je o čem se většinou bavíme my
 - Ochrana dat před jejich ztrátou např. (zálohování) vysoká dostupnost
 - Ochrana dat před jejich odcizením
 - Ochrana dat před jejich zneužitím



Počítačová bezpečnost



GDPR povinnost chránit data + práva

- Povinnosti správců
 - Ochrana dat
 - Interní hrozby
 - Externí hrozby
- Práva uživatelů

Koncept a motivace útočníků současnosti

The Economics of Computer Hacking Peter T. Leeson

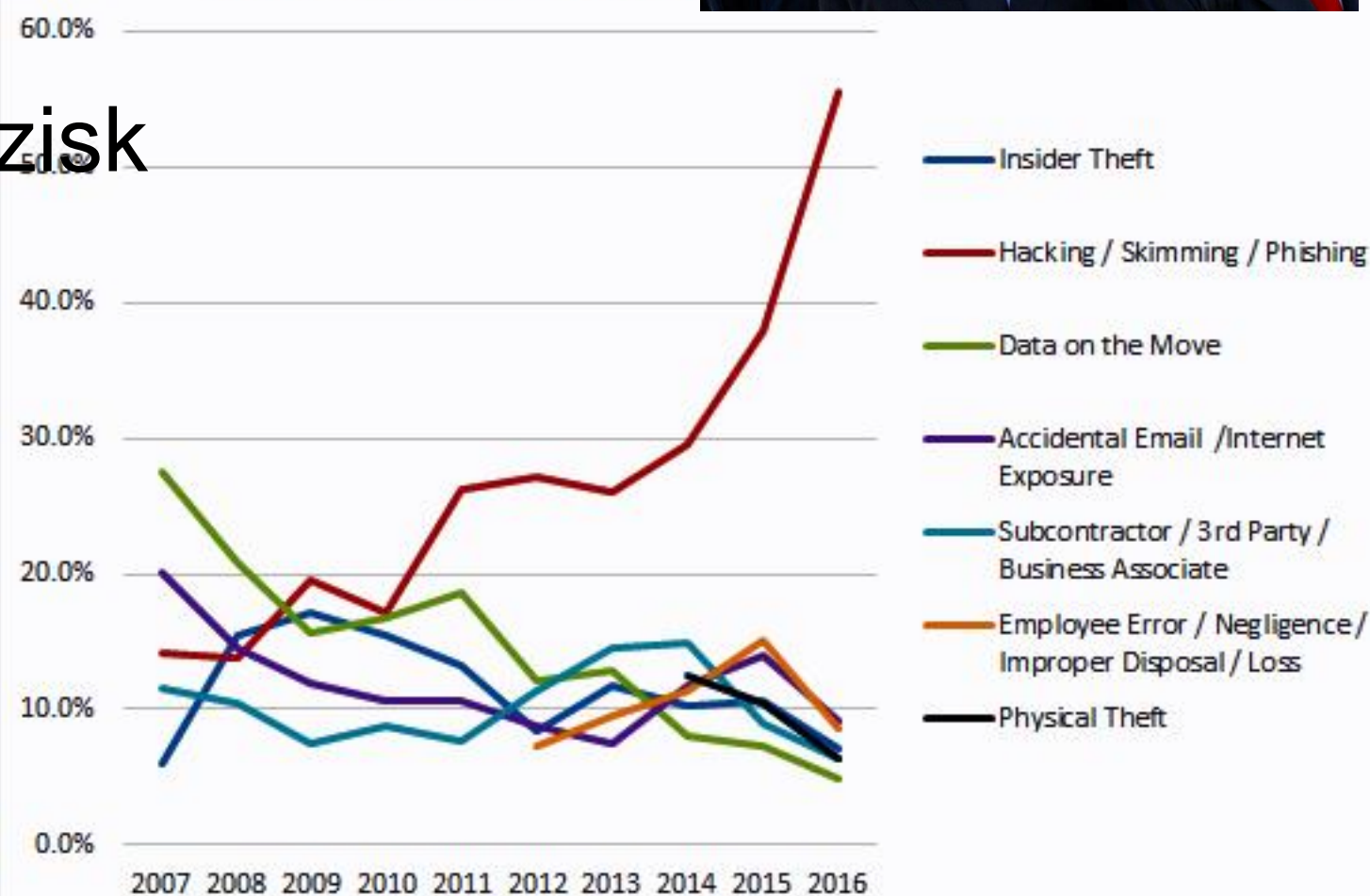
Jediná motivace nyní je zisk

Current prices on the Russian underground market:

- Hacking corporate mailbox: \$500
- Winlocker ransomware: \$10-20
- Unintelligent exploit bundle: \$25
- Intelligent exploit bundle: \$10-\$3,000
- Basic crypter (for inserting rogue code into a benign file): \$10-\$30
- SOCKS bot (to get around firewalls): \$100
- Hiring a DDoS attack: \$30-\$70/day, \$1,200/month
- Botnet: \$200 for 2,000 bots
- DDoS botnet: \$700
- ZeuS source code: \$200-\$500
- Windows rootkit (for installing malicious drivers): \$292
- Hacking Facebook or Twitter account: \$130
- Hacking Gmail account: \$162
- Email spam: \$10 per one million emails
- Email spam (using a customer database): \$50-\$500 per one million emails
- SMS spam: \$3-\$150 per 100-100,000 messages



Figure 2: Data Breach Incidents



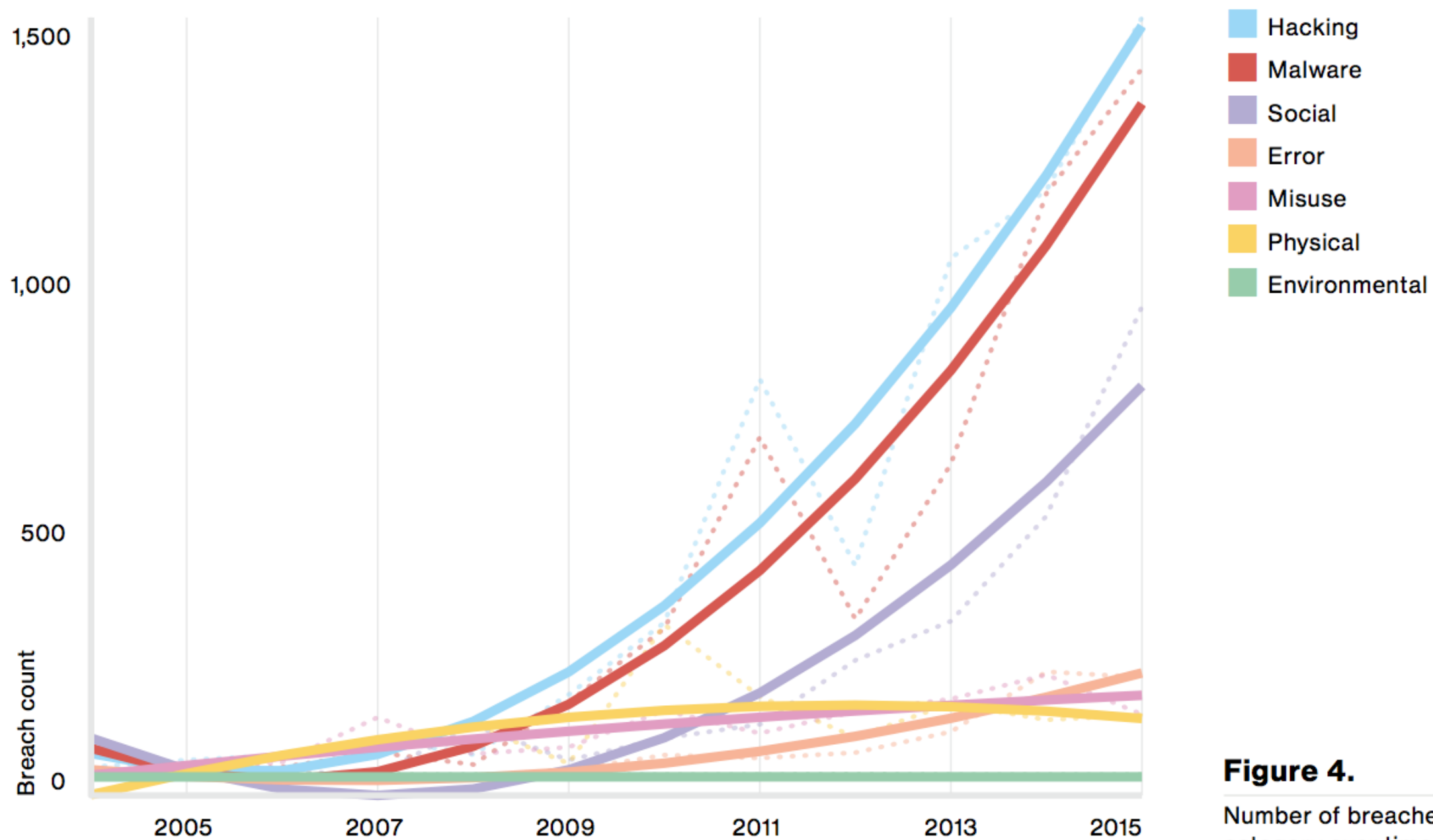


Figure 4.
Number of breaches per threat action category over time, (n=9,009)

Time to compromise and exfiltration.

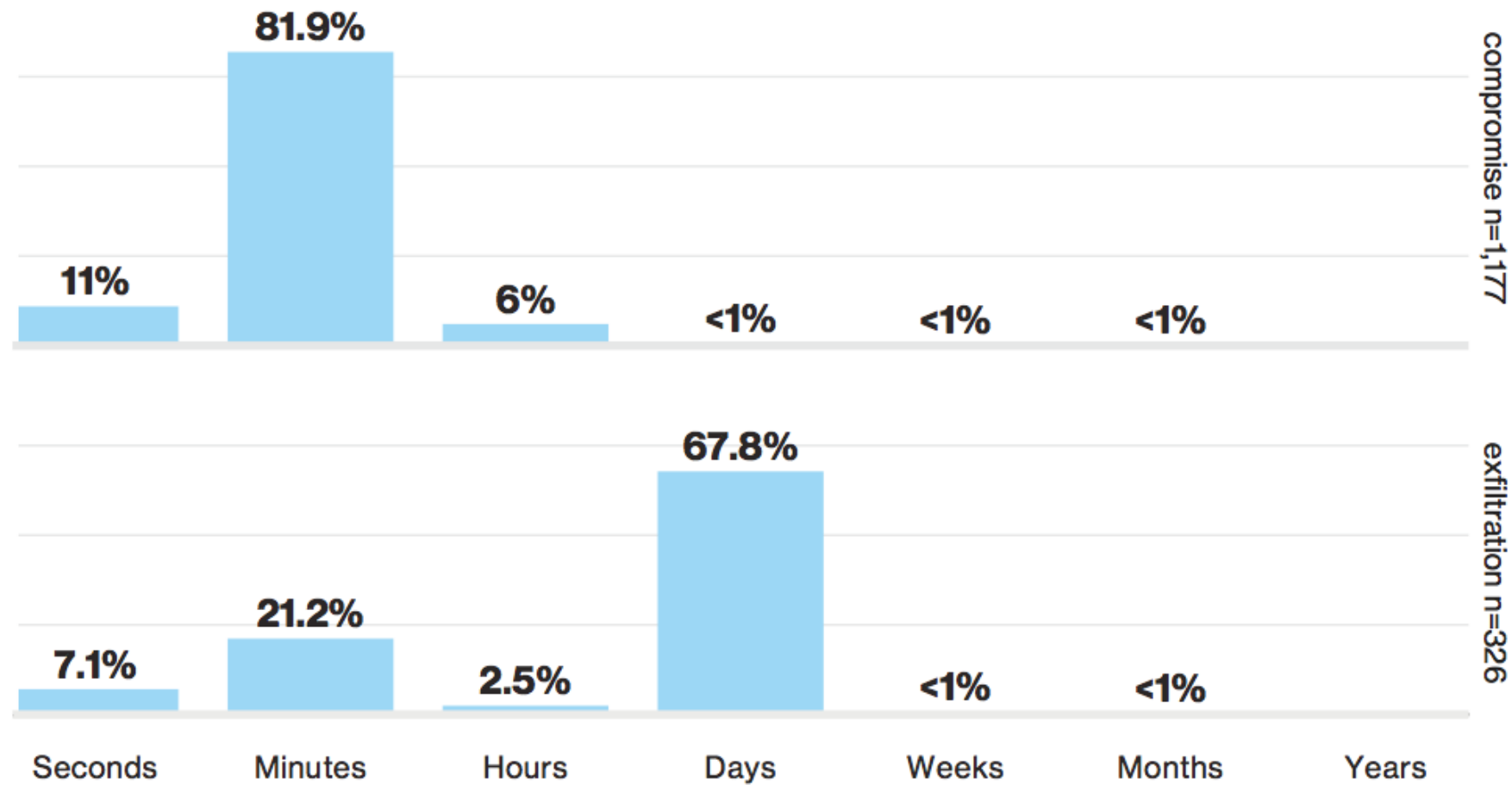


Figure 7.

Time to compromise and exfiltration.

Detection x Compromise % day or less

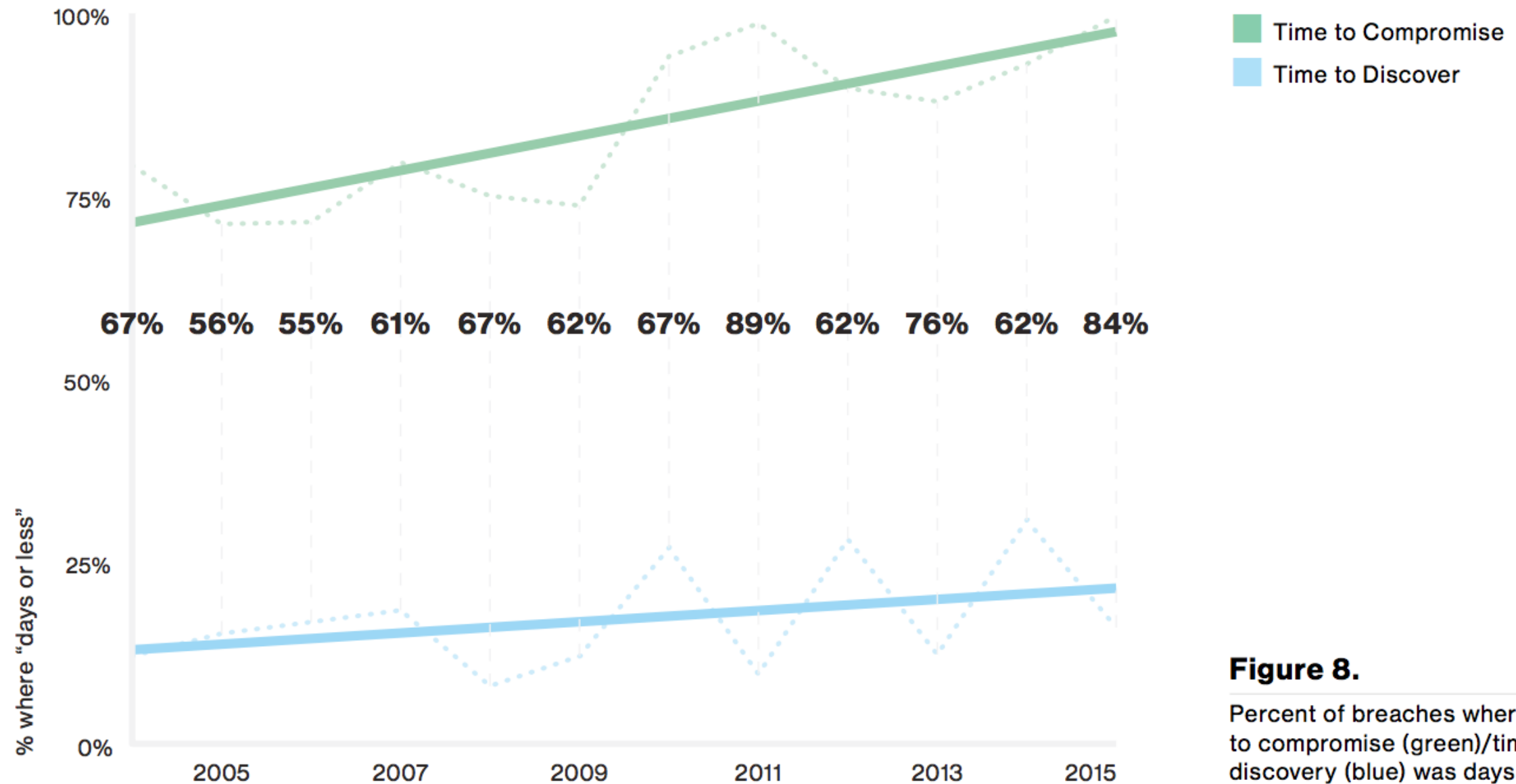
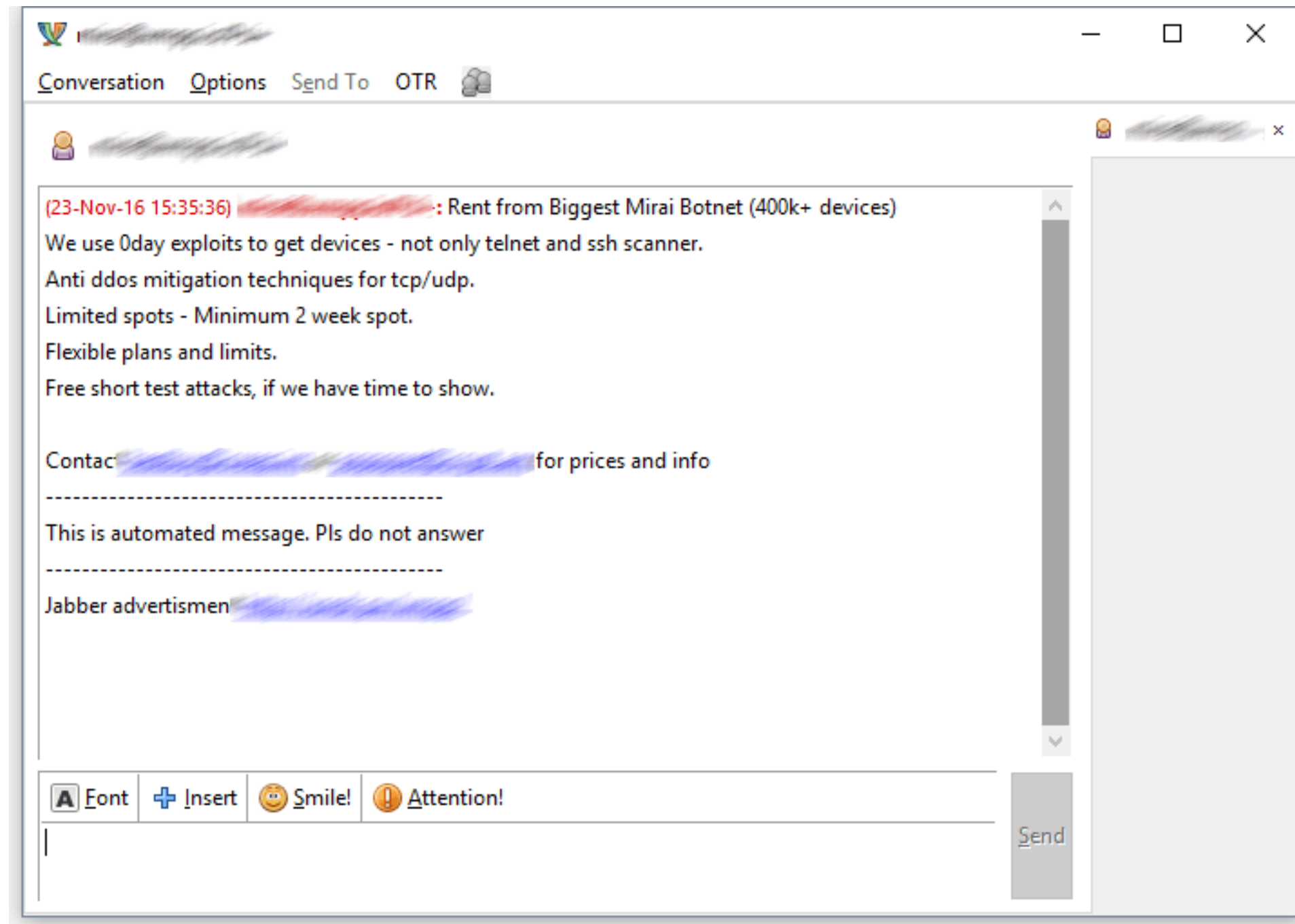


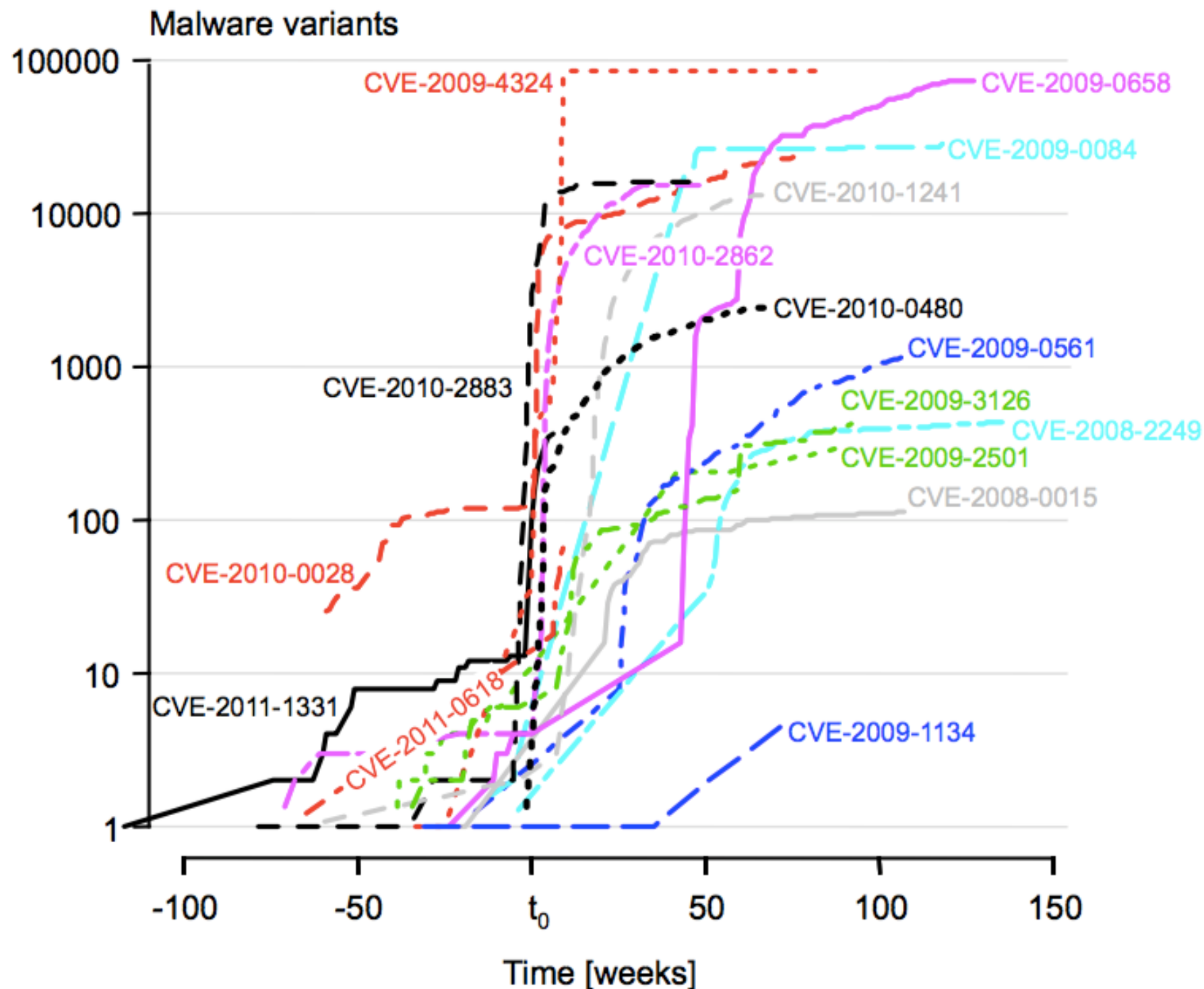
Figure 8.

Percent of breaches where time to compromise (green)/time to discovery (blue) was days or less

Botnet for rent



0-day útoky pohled v čase



Překážka zavedení bezpečnostních technologií

Největší překážky zavedení pokročilých bezpečnostních procesů a technologií

2015 (n=2432)



Věčný souboj

- Útočník
 - Zrychlení vývoje
 - Zdokonalení technologií
 - Zlevnění zdrojů
- Obránce
 - ROI
 - Projekty
 - Stávající bezpečnostní řešení

Funkční modely?

- Místo detekce Prevence
- 0-trust model
- Security by design??
- Privacy by design je pouze zlomek

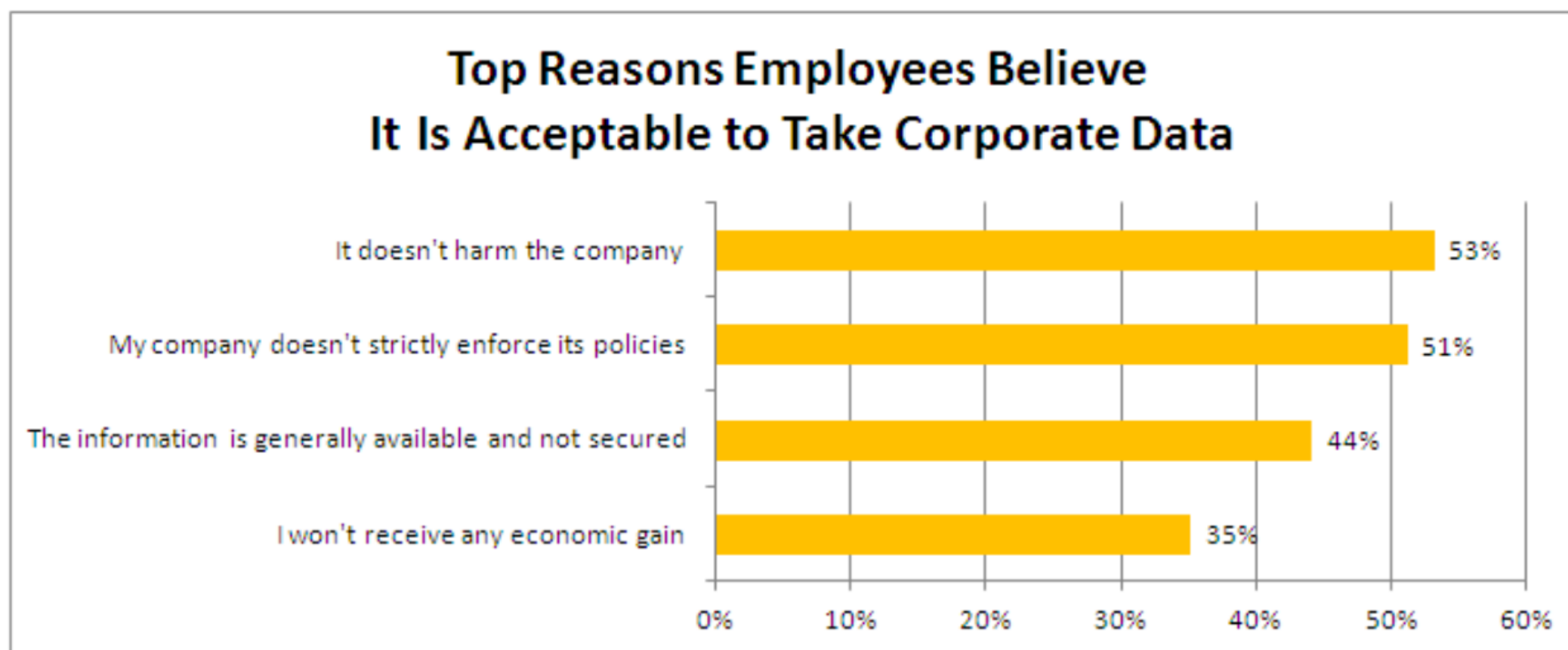
Security je o nejslabším článku

- Vždy se najde nějaký způsob
- Snahou však je nebýt zcela bez ochrany
- Mít lepší ochranu/obranu než ostatní
- Vědět co chráním, jakou to má cenu

Co pomáhá?

- Zaměstnanci
 - Informovanost, měřitelnost
- Útočníci
 - Prevence
 - Nové technologie, nespoléhat pouze na detekci, vidět znamená mít šanci

Co si myslí zaměstnanci o firemních datech



2016 Internet Security Threat Report



A New Vulnerabilities Found Discover in 100 Million Fake Technical Support Ransom We Scams Blocked Cyber c on Cyber scammers now make you call them

An extreme to ensnare device that found new Symantec smart wa The Fake technical support scams have evolved from cold-calling unsuspecting victims to the attacker fooling victims into calling them directly. Attackers trick people with pop-up error alerts, thus steering the victim to an 800 number where a “tech support rep” attempts to sell the victim worthless services. In 2015, Symantec blocked 100 million of these attacks. s most likely out the year. to targeted employees risk.

Vulnerabilities Found in Three Quarters of Websites *Web administrators still struggle to stay current on patches*

There were over one million web attacks against people each day in 2015. Cybercriminals continue to take advantage of vulnerabilities in legitimate websites to infect users, because website administrators fail to secure their websites. Nearly 75 percent of all legitimate websites have unpatched vulnerabilities, putting us all at risk.

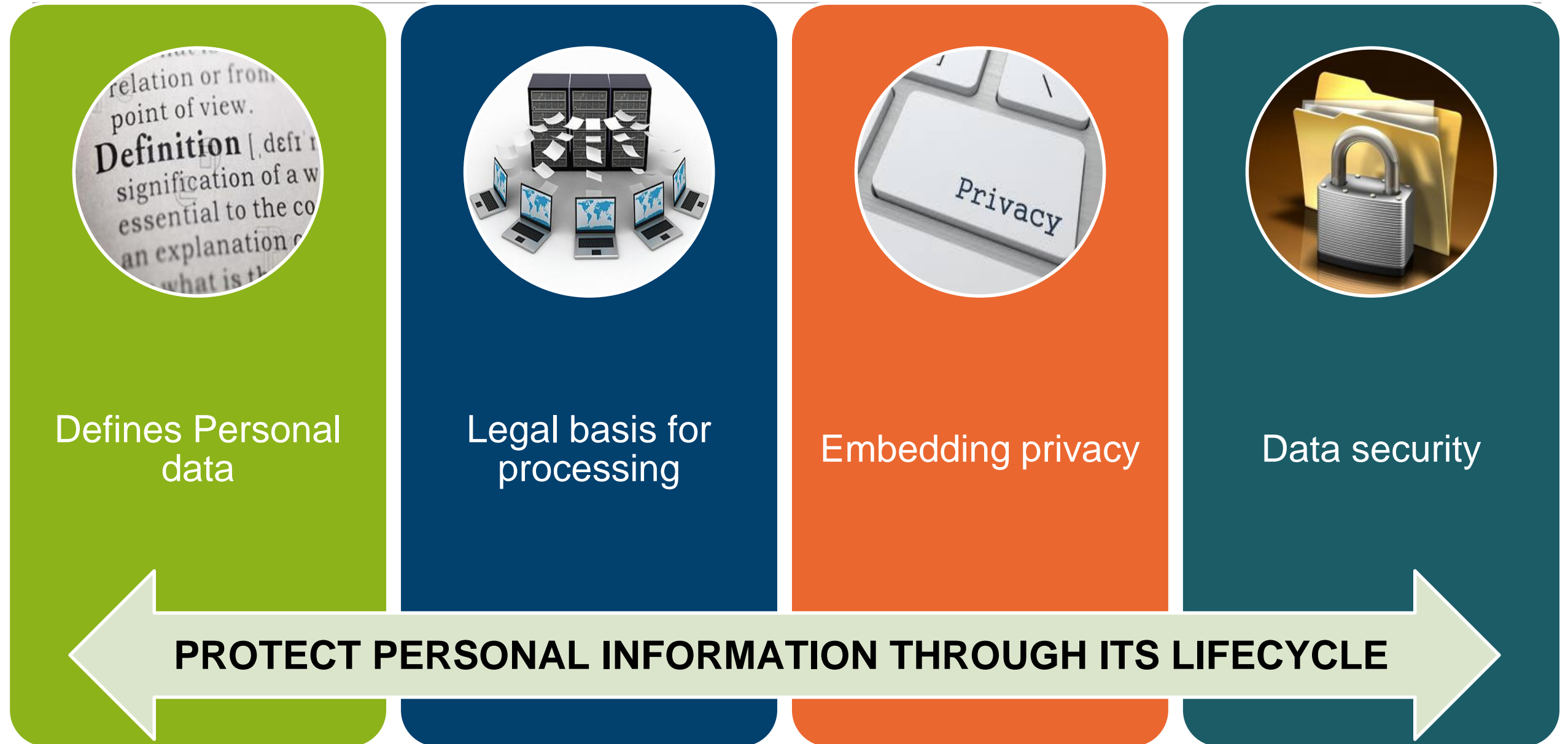
Scams Blocked *Cyber scammers now make you call them*

Fake technical support scams have evolved from cold-calling unsuspecting victims to the attacker fooling victims into calling them directly. Attackers trick people with pop-up error alerts, thus steering the victim to an 800 number where a “tech support rep” attempts to sell the victim worthless services. In 2015, Symantec blocked 100 million of these attacks.

LEARN MORE

For more information about the cyber threat landscape and the potential impact it has against you and your organization, download the 2016 Symantec Internet Security Threat Report at: www.symantec.com/threatreport

Scope of the GDPR



GDPR – Úniky dat

AMS

EMEA

APJ



Is Barbie spying on your children? Top toy firms fined \$835,000 for tracking online activity and collecting personal data of children under 13

- Viacom, Mattel, Hasbro and JumpStart fined for tracking kids online
- Two-year probe was conducted by New York Attorney General's office
- Must \$835,000 and regularly check websites for tracking technology

By ASSOCIATED PRESS and STACY LIBERATORE FOR DAILYMAIL.COM
PUBLISHED: 20:04, 13 September 2016 | UPDATED: 07:36, 15 September 2016



Gone are the days when children being out past dark was a parent's worst fear; now they have to worry about smart toys tracking their child's every move.

After a two-year probe, Viacom, Mattel, Hasbro and JumpStart have been ordered to pay \$835,000 in fines for tracking and collecting personal data of children online.

All four companies allowed tracking technology on their websites, which violates the Children's Online Privacy Protection Act that limits marketing to children under 13.

Scroll down for video



Security

Tesco would face fines of up to £1.9bn under GDPR for Tesco Bank breach

Entire Tesco group would be in the firing line - with demands for more payouts on top from class-action lawsuits

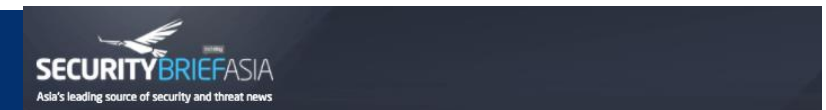
Graeme Burton

@graemeburton

08 November 2016



2 Comments



TAGS

Data breach, Eretail, Blackberry, Ecommerce

Protect your data at all costs, if this latest scandal is anything to go by

JANUARY 17, 2017 9AM | SHANNON WILLIAMS

Protect your data at all costs, if this latest scandal is anything to go by.

That's the takeaway lesson from a recent news item appearing on the [Sydney Morning Herald website](#) this morning, detailing how a naughty former employee exported her company's entire customer database before she exited the door.

According to an article by [Jessica Sier](#), online fashion e-retailer Showpo is suing Black Swallow, a similar e-commerce business, which Showpo claims has used the database to market itself as an affiliate of Showpo.

The article says former Showpo employee Melissa Aroutunian exported the 306,000-strong customer database before she left the company, and passed it on to Black Swallow.

Snaha vše utajit již nebude fungovat

Chovanec chce vyšetřit, kdo kyberútok na MZV prozradil veřejnosti

2. 2. 2017 13:05

Ministr vnitra Milan Chovanec (ČSSD) trvá na důsledném vyšetření toho, odkud na veřejnost unikly informace o hackerském útoku na české ministerstvo zahraničí. Šéf diplomacie Lubomír Zaorálek (ČSSD) o útoku informoval v úterý poté, co o něm napsala některá média. Chovanec dnes novinářům řekl, že státní orgány o činnosti hackerů věděly s předstihem a předčasný únik může ohrozit vyšetřování. Zprávu přinesla ČTK.



Sdílet To se líbí 88 lidem.



Hackeri získali z ministerstva zahraničí 7 000 dokumentů. Včetně citlivých informací

1. 2. 2017 22:06

Hackerský útok na ministerstvo zahraničí trval nejméně rok. Útočníkům na počítačovou síť se za tu dobu podařilo ukrást více než 7 000 dokumentů, některé z nich obsahovaly citlivé informace. Jejich držitel může podle Národního centra pro kybernetickou bezpečnost (NCKB) získat nad Českem strategickou výhodu. S odvoláním na zprávu NCKB to dnes napsal server Info.cz. Zprávu převzala ČTK.

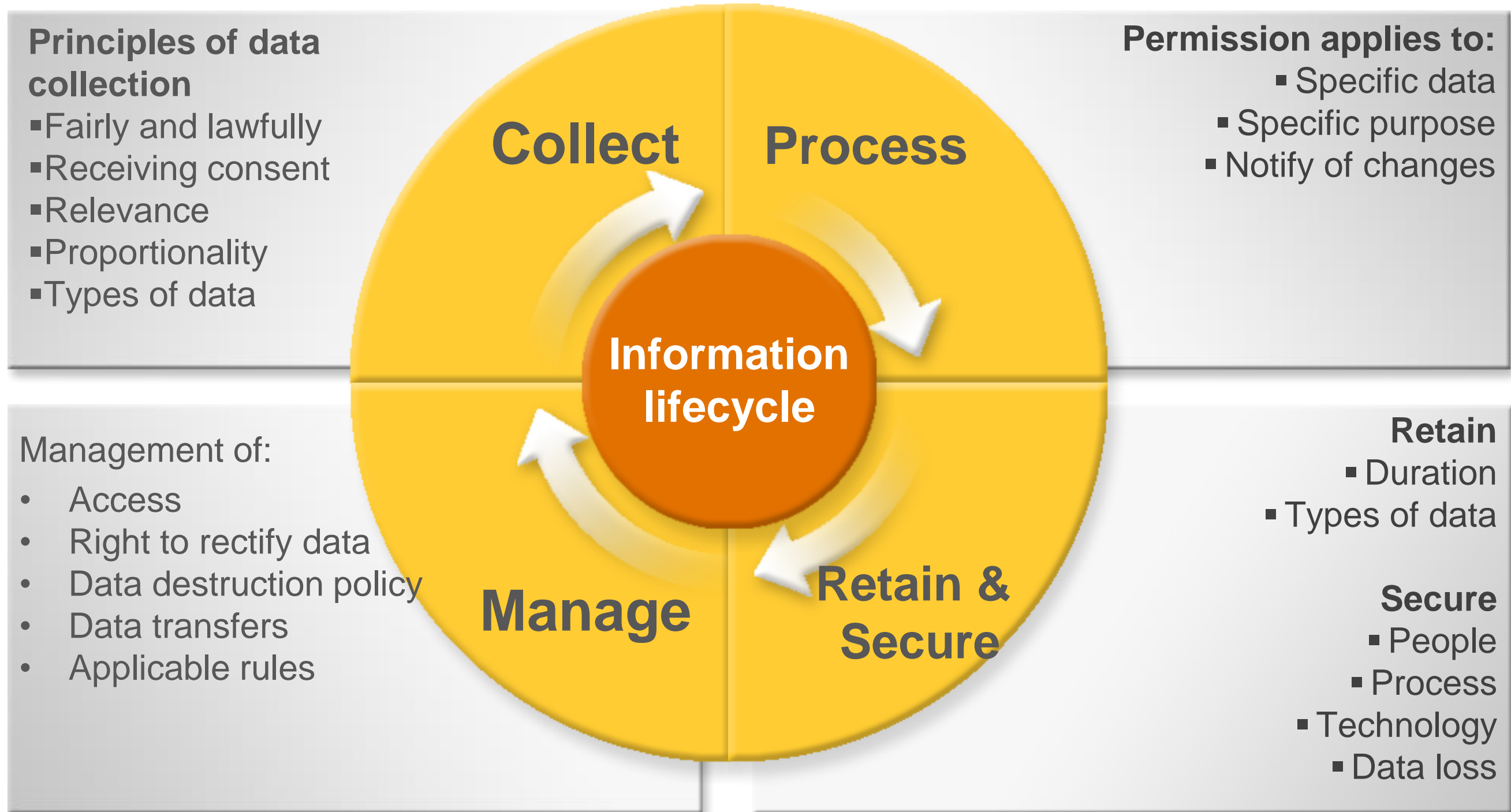


20



1.11.2016

GDPR is about data governance



GDPR



za 5
minut 12

aneb **ČESKÁ REPUBLIKO,
PROBER SE!**



Obecné nařízení na ochranu osobních údajů (GDPR) vstoupí v členských zemích EU v platnost 25. května 2018. Čas do příštího jara se může zdát jako dlouhá doba, opak je však pravdou. České státní ani soukromé organizace nejsou na tuto novou normu připraveny a čas to napravit se krátí.

Na příkladu fiktivní české organizace o 1 000 zaměstnancích podléhající režimu zákona o veřejných zakázkách, která by započala s příslušnými kroky neprodleně v únoru letošního roku, si můžeme ukázat, že i při optimistickém odhadu časové náročnosti kroků, které vedou k souladu interního systému ochrany osobních údajů s GDPR, není pravděpodobné úspěšně dokončit proces této přípravy dříve než právě v květnu příštího roku.

GDPR není bezzubá norma. Oproti pokutám dosud ukládaným za porušení pravidel pro ochranu osobních údajů příslušnými orgány ČR přichází GDPR s pokutami do výše 20 milionů Euro nebo do výše 4 % z celosvětového ročního obrátu. Při zkoumání porušení GDPR je ale polehčující okolností, pokud daná organizace alespoň činí kroky pro omezení rizik v oblasti ochrany osobních údajů – tedy pokud s přípravou alespoň začala.

Máte dotazy k GDPR?

Zavolejte nám:

Petr Zahálka, tel.: +420 602 354 836
specialista kybernetické bezpečnosti, Avnet,

DATOVÝ AUDIT

Časová náročnost: 6 – 12 měsíců

Datový audit dává odpovědi na otázky, co, kde, jak a proč organizace dělá s osobními údaji. Pro většinu velkých českých organizací je problém tyto otázky kvalitně zodpovědět vlastními zaměstnanci. Bez těchto odpovědí není možné kvalitně poptat nové řešení interního systému nakládání s osobními daty. Proto je třeba, aby si organizace nechaly zpracovat datový audit. Tento proces v případě organizace s 1 000 zaměstnanci zahrnuje vypsání záměru, vyhlášení veřejné zakázky na zpracovatele datového auditu, jeho výběr, provedení samotného auditu a zpracování závěrů. Takový proces trvá přibližně 6 – 12 měsíců.

TENDR NA SW A HW

Časová náročnost: 6 měsíců

Příprava zadávací dokumentace pro takto složitou zakázku na základě výsledků datového auditu je sama o sobě časově náročným úkolem, obzvlášť v případě aplikace zákona o veřejných zakázkách. Ten sice v případě otevřeného řízení pro nadlimitní veřejnou zakázku umožňuje stanovit lhůtu pro podání nabídek na 52 dny, současně ale zadavatel musí mít na paměti, že lhůta by měla být adekvátní složitosti zakázky. Pro hledání komplexního řešení v oblasti IT se navíc hodí institut tak zvaného soutěžního dialogu, který je pochopitelně časově náročnější. I po případném výběru dodavatele je pak třeba počítat s možností námitek ze strany neúspěšných uchazečů. Zkušenost ukazuje, že průměrná doba od vypsání několikamilionové veřejné zakázky v oblasti IT do podpisu smlouvy s dodavatelem činí 6 měsíců.

VÝBĚR DPO

Časová náročnost: pravděpodobně značná

V případě státní správy a soukromých organizací pravidelně a systematicky zpracovávajících velké objemy osobních údajů je podle GDPR povinné vytvoření pracovní pozice pověřence pro ochranu osobních údajů (Data Protection Officer – DPO). Tato pozice přitom klade na člověka, který ji bude zastávat, mimořádné nároky, neboť v sobě musí kombinovat hluboké znalosti o procesech v instituci se znalostmi a rozhledem v oblasti IT. Zejména ve státních a veřejných institucích takové lidi scházejí. Odhady mluví o 1 000 až 1 500 scházejících profesionálech v této oblasti ve státních a veřejných institucích v ČR. Obsazení tohoto postu bude trvat nějakou dobu. Jeho neobsazení může zpozdit přípravné činnosti a v květnu 2018 se bude jednat o nelegální stav.

IMPLEMENTACE NOVÉHO SYSTÉMU

Časová náročnost: 3 měsíce

I po vysoutěžení nového softwaru a hardwaru pro zajištění adekvátní míry ochrany osobních údajů je třeba uvést tento nový systém v život, spolu s úpravou interních směrnic, procesů a proškolením zaměstnanců v oblasti ochrany dat. Spuštění takto rozsáhlé změny ve velké organizaci může stěží trvat méně než tři měsíce.

PRIVACY IMPACT ASSESMENT

Časová náročnost: 6 měsíců

Každý projekt, jehož součástí bude zpracování velkého objemu osobních údajů, který bude spuštěn po 25. květnu 2018, bude muset splňovat požadavky GDPR. Jelikož ochrana je zejména otázkou designu jakéhokoli IT řešení (dodatečně naprogramované ochranné prvky jsou finančně několikanásobně náročnější a nejsou dostatečně účinné), je třeba provést vyhodnocení dopadů na soukromí jednotlivce ještě před začátkem přípravy projektů, které mají být realizovány v době platnosti GDPR. Tento čas tedy můžeme symbolicky přičíst k celkové době přípravných činností, které musejí ve velkých organizacích proběhnout v nejbližší době.

Děkuji za pozornost

- Petr Zahálka
- Techdata
- petr.zahalka@techdata.com
- +420 602 354 836