



DIVELIT



DRIVEN BY INNOVATION
DELIVERED BY PEOPLE

„Stejné chyby, stejné známky“

–

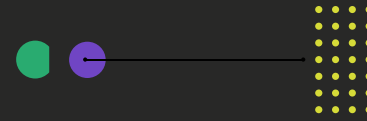
Sonda do reality kybernetické
bezpečnosti firem a organizací





Disclaimer

- * Nemáme univerzální pravdu
- * Vzorek je specifický – zjištění nemusí být vždy platná



Obsah

- 1.) Co jsme dělali?
- 2.) Co se nám ukázalo?
- 3.) Na čem pracovat?



Koncept

- kontinuální aktivita
- cca hodinový rozhovor
- zaměření částečně přizpůsobeno respondentům
- terapeutické prvky 😊



Vzorek (průměry)

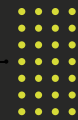
- primárně soukromý sektor (s výjimkou několika státních institucí)
- obvykle od 20 po 250 zaměstnanců
- technologické, výrobní firmy, poskytovatelé služeb



Charakteristika organizací – specifita vzorku

Typicky naši respondenti disponují pokročilým technickým know-how v nějaké oblasti

Většina ze zapojených organizací je v tuto chvíli blízka vývoji produktů s digitálními prvky



Rozdílná vlastnická struktura

- ryze české firmy
- dceřiné společnosti s vedením v zahraničí apod.
- nemocnice / úřady



Firmy s matkou v zahraničí

Rozdílná míra autonomie

„Sami si nemůžeme vyměnit ani toner v tiskárně.“

„Jedeme si podle sebe.“

Obecný trend

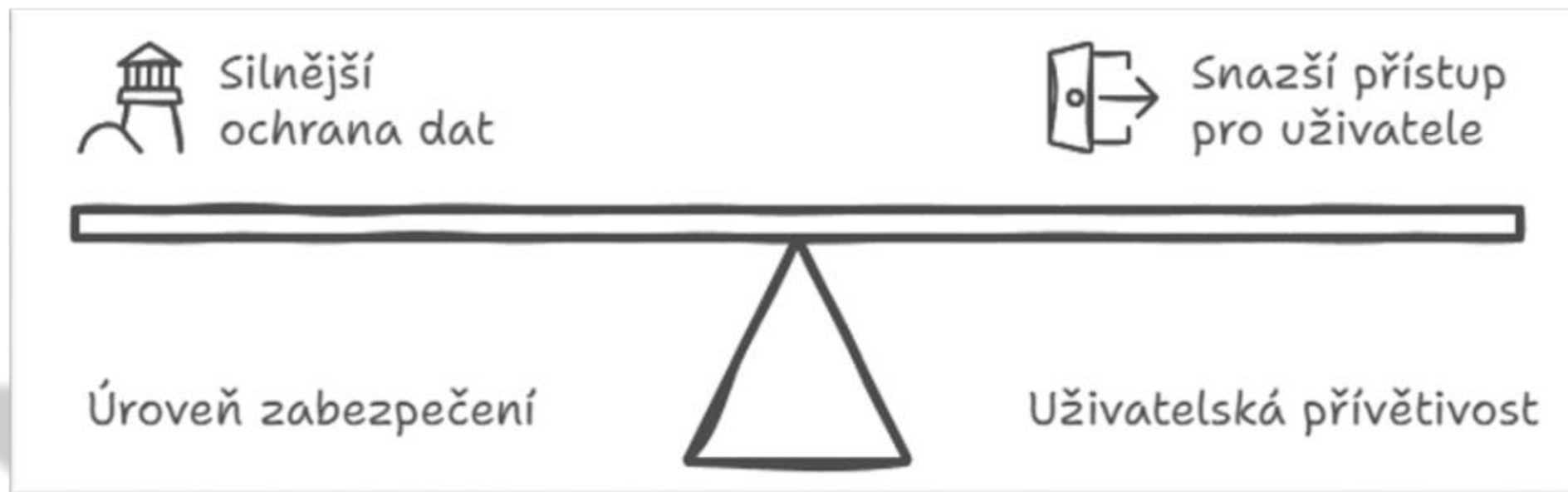
Mnohem více procesů souvisejících s oblastí kyberbezpečnosti

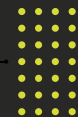
Pokročilejší úroveň zabezpečení bez negativního přijetí ze strany zaměstnanců

„Respekt“ k oborovým standardům – snaha dělat to správně a **reálně**

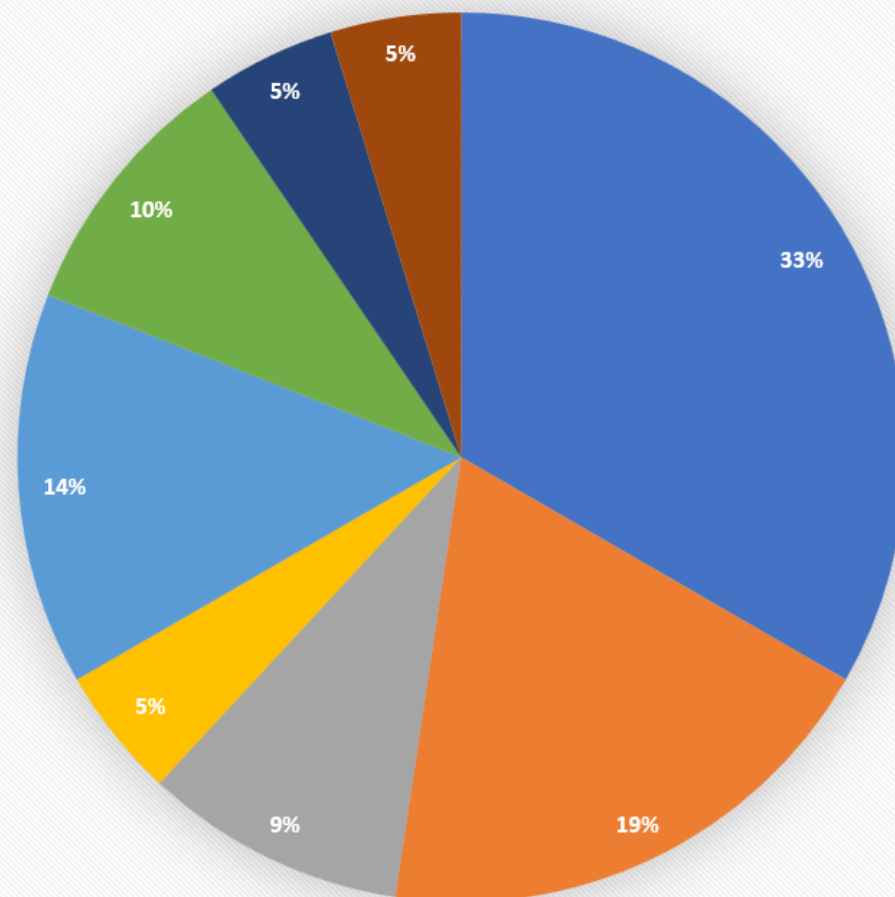
Firemní kulturu je třeba budovat (strategicky a postupně)

Opatření „jako samozřejmost“ vs. „Všichni vývojáři musí mít lokálního admina“





Respondenti – delegované osoby

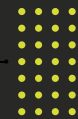


■ Head of IT ■ CEO ■ CTO ■ CFO ■ Tým lidí ■ R&D director ■ Quality Manager ■ Cybersecurity Manager

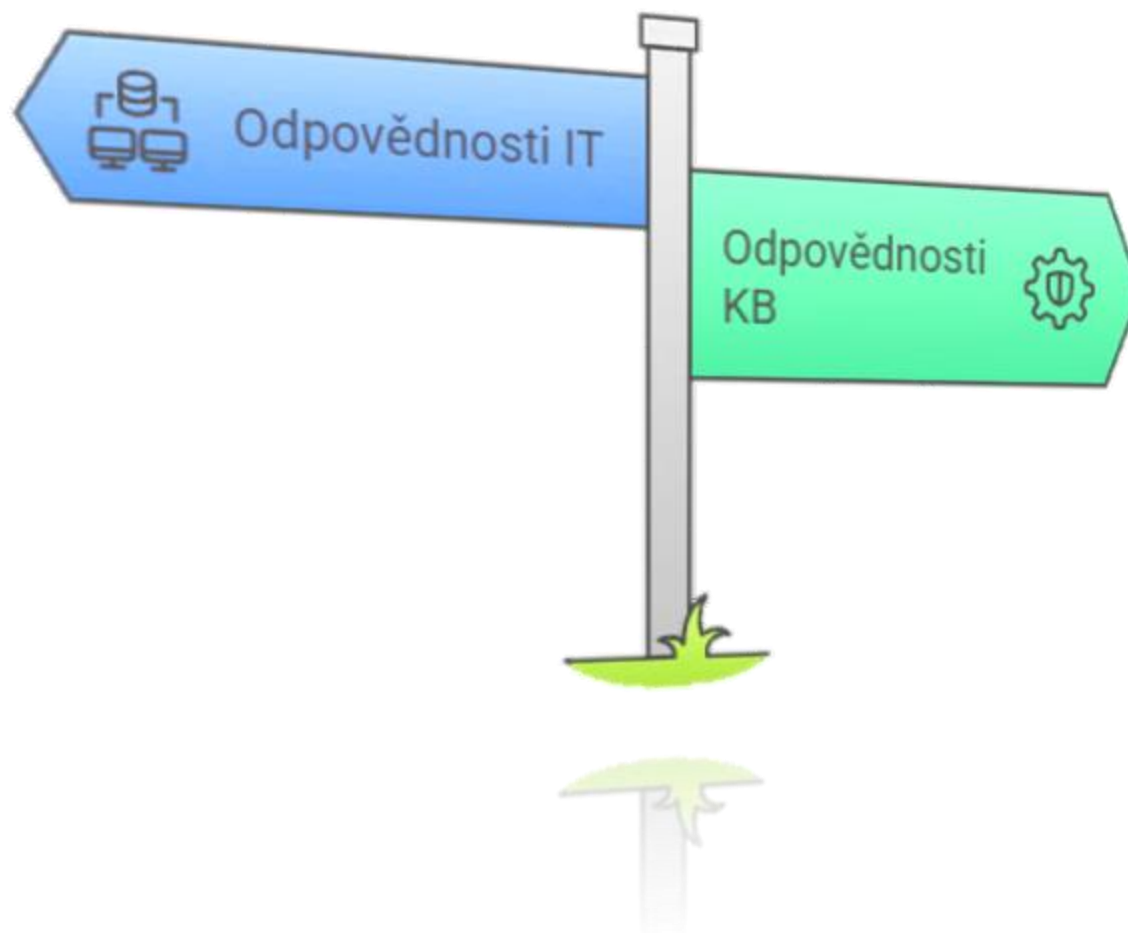


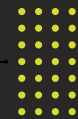
Kybernetická bezpečnost není záležitostí IT





Odpovědná osoba



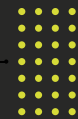


Často se říká, že firmy podceňují svou hodnotu pro útočníka

Přístup „**nás se to netýká – pro nikoho nejsme zajímaví**“ – to být ani nemusíte!

Schizofrenie „po česku“

Svoji hodnotu si uvědomujeme (alespoň to tvrdíme), z pohledu ochrany ale nic moc neděláme, protože „na to není prostor“

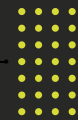


Vzdělávání / školení zaměstnanců

Doporučuje 11 z 10 odborníků

Pravidelně realizují tak 2 z 10 firem





I přes to, že největší obavou je obvykle selhání lidského faktoru

„Lidi jsou věčný problém.“

„Lidi jsou“

„Říkáte jim neklikejte, oni přijdou ze školení ... a kliknou.“



Tudy spíše ne

„Bavili jsme se o tom, hledáme, jak řešit ...“

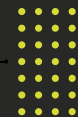
Phishingová kampaň a následný shaming

„Řešíme dle aktuální situace“ == Jednou jsme zmínili na poradě

E-mail jednou za měsíc

„Spoléháme na povědomí uživatelů ...“

„Máme e-learning, stačí to proklikat.“



Tohle by bylo lepší

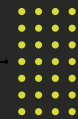
„Zážitková“ školení – pokud nejde jen o buzzword → mohou mít aha efekt

e-learning s průběžným vyhodnocováním a úpravou dle dosažených výsledků

Ideální je kombinace přístupů a forem, promítnout bezpečnost i mimo kontext pracovní doby

Pracovat specificky s konkrétními skupinami uživatelů

Striktní dodržování **I U VEDOUCÍCH ZAMĚSTNANCŮ**

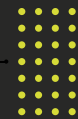


Legislative a standardy – „Rozumím, ale nechápu.“



Máte zavedena opatření? A mohla bych je vidět?





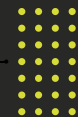
Legislativní požadavky? Řešíme ...

NIS2 na klíč

Analýzy bez součinnosti

Utrácení bez užitku (pro dobrý pocit?)

Formální výstupy bez dopadů



Standardizace – relevance a uchopení

Máme ISO 27001 a nebojíme se ho použít ignorovat

Vůbec nic se nezměnilo

„Jde tam napsat cokoliv“

„Jde tam zdůvodnit cokoliv“

„Chceme dělat KB odspodu“

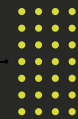
přehled o vlastním prostředí

zavedená opatření a (re)akční plány

plán RELEVANTNÍCH investic!

garance směrem k zákazníkům

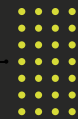
Když už se to děje, tak ať z toho něco máte.



Čím víc papírů, tím víc adidas



**Srozumitelnost, přehlednost,
dostupnost a aktuálnost!**



Outsourcing jako sprosté slovo?

(Ne)znalost prostředí vs. nezávislý pohled

Budování interních kapacit vs. externista

Jde o „dodání projektu“ nebo např. mentoring?

***I s externisty lze budovat bezpečnost uvnitř firmy.
Jen nesmí bezpečnost odejít s nimi.***



Reakční plány

„Máme, někde jsou.“

„Máme, jsou v cloudu.“

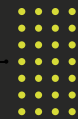
„Máme, v obecné rovině.“

„Nemáme, ale lidi ví, co mají dělat.“

Sepsat minimum:

- * Kontaktní matice
- * Odpojení elektriny
- * Nedostupnost klíčových systémů
- * Postup obnovy záloh

...



Co si z toho vzít?

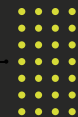
Kybernetickou bezpečnost řešte kvůli fungování businessu.

Nenakupujte zázračná řešení.

Nejprve identifikujte, co už máte / děláte a vytvořte informovaný plán rozvoje.

Bezpečnost bude třeba odpracovat ☹️

Jde o proces, nikoliv jednorázový projekt.



Rádi se potkáme i s Vámi

Matěj Očenášek
CEO

+420 774 109 076
ocenasek@divelit.cz
www.divelit.cz



DIVELIT



Jaroslav Krbec

Product Manager | Cybersecurity Specialist

+420 725 830 008
krbec.jaroslav@divelit.cz
www.divelit.cz



DIVELIT

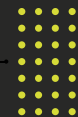


DIVeLIT

DRIVEN BY INNOVATION
DELIVERED BY PEOPLE



27



Díky.