ALEF

Uvědomělí zaměstnanci: nejlepší bezpečnostní opatření

Jan Kopřiva

jan.kopriva@alef.com

ALEF CSIRT

TLP: WHITE

Člověk vs. bezpečnost v číslech

- 27% úniků dat je způsobeno uživatelským pochybením
- 4% uživatelů kliknou na odkaz v jakémkoli phishingu
- Až 96% útoků je realizováno s pomocí phishingu
- 1 z 13 webových požadavků vede k malwaru
- 41% organizací má přes 1000 citlivých souborů volně přístupných všem uživatelům

Security awareness a plány vzdělávání

- Program pro zvyšování uživatelského povědomí
- Plán vzdělávání všech rolí v organizaci
  - Specifický obsah pro jednotlivé role (uživatel vs. IT specialista)
  - Specifická forma pro jednotlivé role (CEO vs. účetní)

Security awareness pro uživatele

- Obsah
  - Interní bezpečnostní dokumentace
  - Externí regulace
  - Nejpodstatnější hrozby a metody ochrany
- Forma
  - CBT (osobní školení, onboarding prezentace,…)
  - E-learning

Security awareness pro C-level role

- Obsah
  - Nejpodstatnější hrozby a metody ochrany
  - Krizové řízení a reakce na incidenty
- Forma
  - CBT (osobní školení, onboarding prezentace,…)
  - Tabletop cvičení
  - Simulace

Bezpečnostní vzdělávání odborných rolí

- Obsah
  - Relevantní bezpečnostní problematika
  - Technické znalosti
- Forma
  - CBT (osobní externí/interní školení)
  - E-learning

ALEF

Jak postupovat?

- Analýza relevantní dokumentace a standardů
- Analýza hrozeb a rizik
- Analýza vzdělávacích potřeb všech relevantních rolí
- Návrh forem, obsahů a period vzdělávání jednotlivých rolí
- Tvorba vzdělávacího plánů
- Tvorba detailních obsahů vzdělávání
- Realizace vzdělávacích aktivit
- Verifikace a vyhodnocení

ALEF

Požadavky na realizační tým

- Zkušenosti s bezpečnostním vzděláváním
- Andragogické/pedagogické vzdělání
- Odborné certifikace dle zaměření tvořeného obsahu
- Trenérské certifikace dle školeného obsahu

ALEF

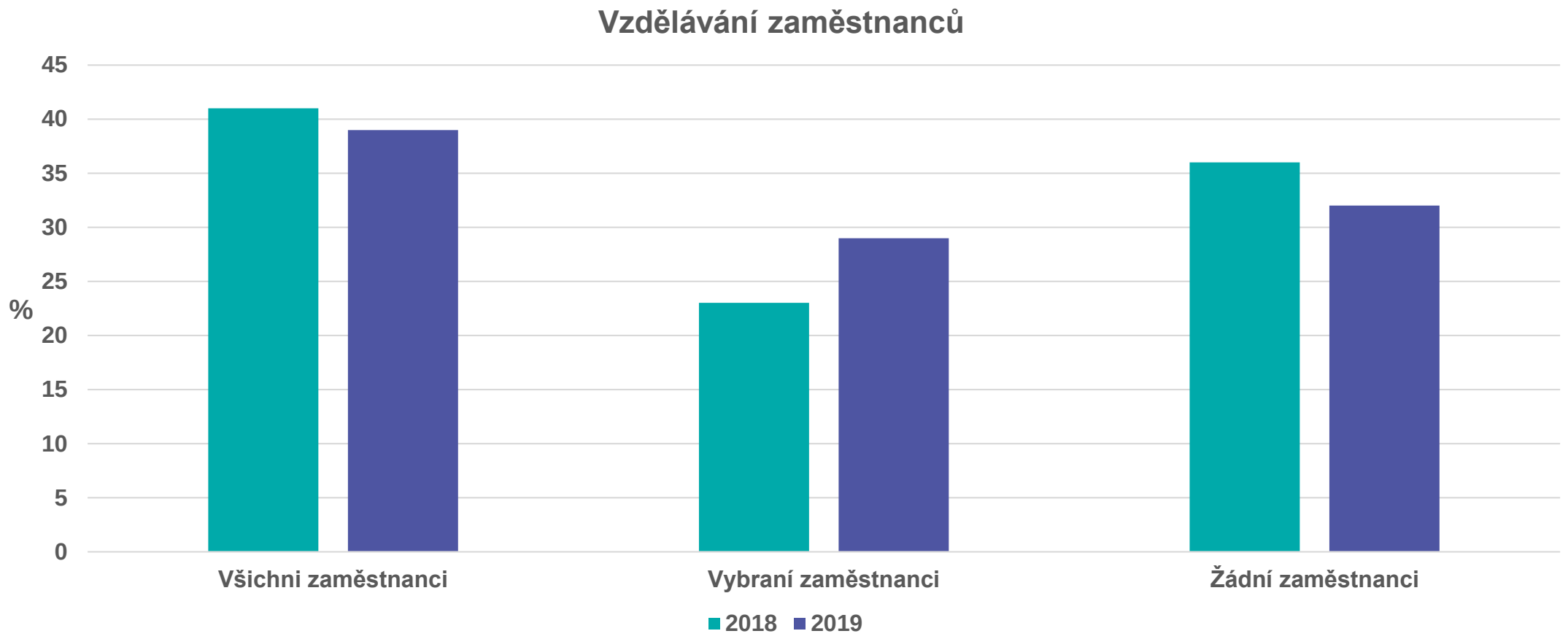
E-learning vs. CBT

- E-learning
  - Vhodný zejména pro masová opakovaná školení s jednotným obsahem
    - Vstupní a periodické školení o základních hrozbách
    - Vstupní a periodické školení o interních směrnicích a politikách
    - Standardizované odborné bezpečnostní vzdělávání
    - …

E-learning vs. CBT

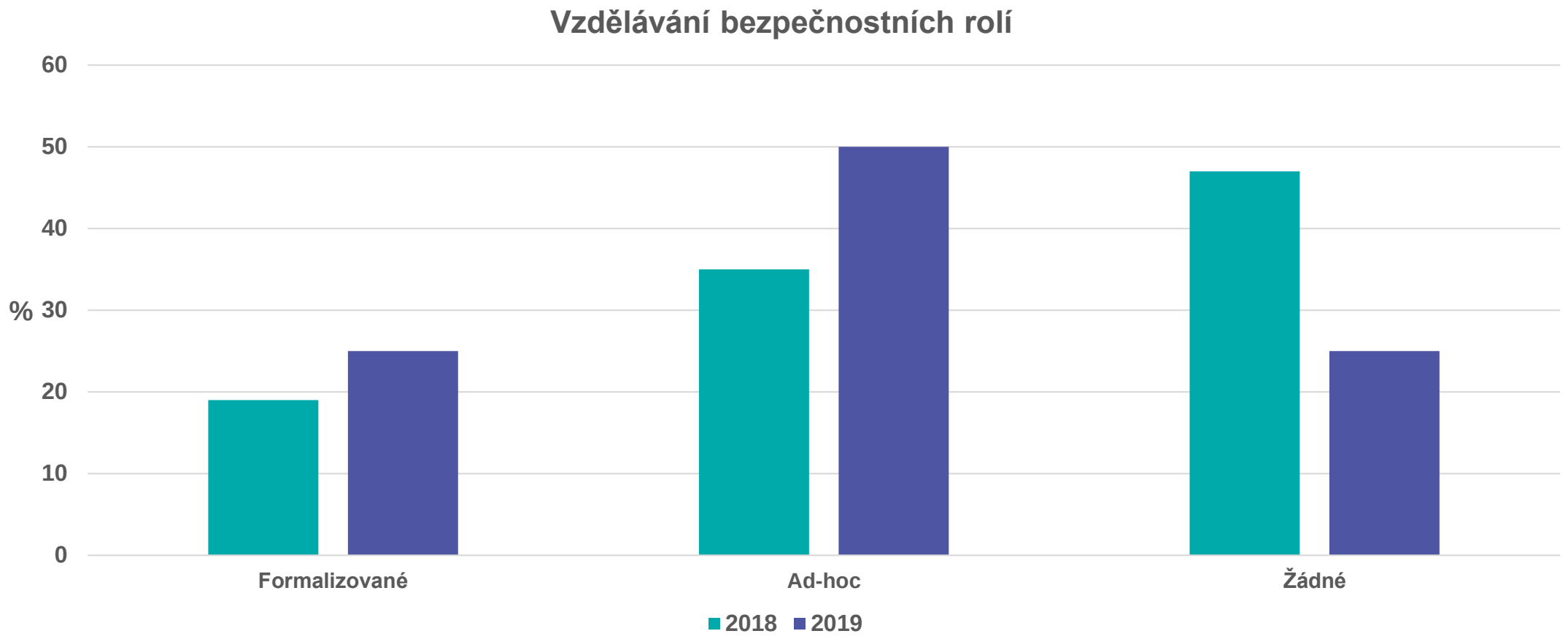
- CBT
  - Vhodný pro odborná školení a školení vyžadující interaktivitu nad rámec skriptovaných událostí
    - Odborná školení pro bezpečnostní tým a IT
    - Školení o hrozbách pro C-level role
    - Praktická školení pro odborné role
    - …

Průzkum v ČR



ALEF

Průzkum v ČR



ALEF

Verifikace a vyhodnocení vzdělávání

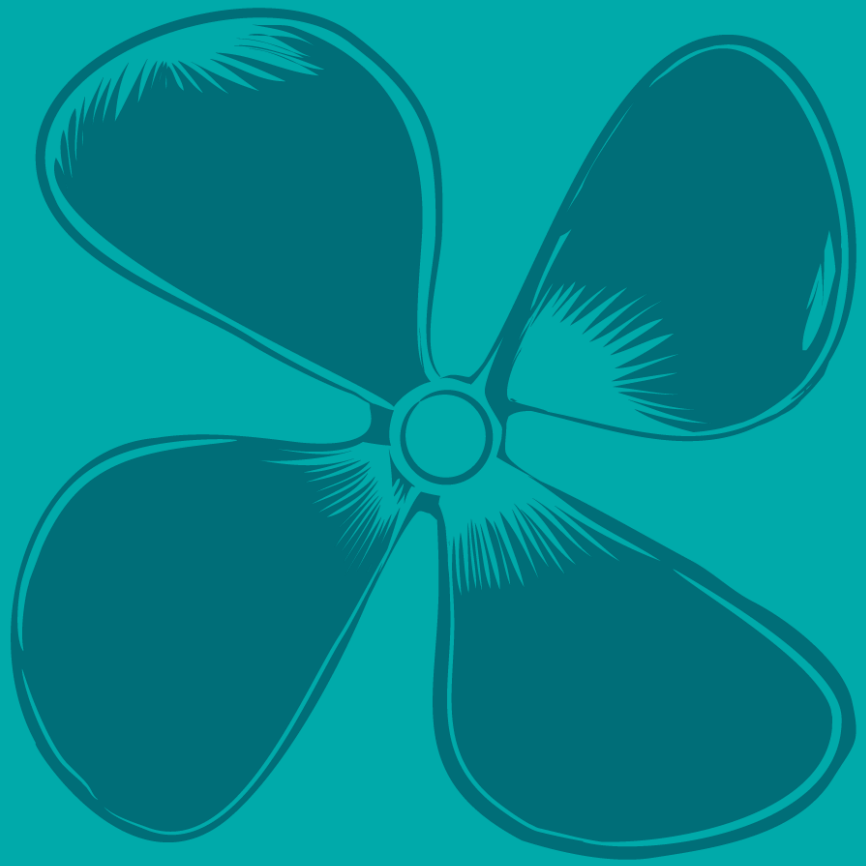
ALEF

Verifikace a vyhodnocení vzdělávání

- Uživatelé
  - Penetrační testy
    - Socioinženýrské (phishing), fyzické
  - Audit
- Odborné role
  - Certifikační zkoušky
  - Testování reakce na incidenty

ALEF

Děkuji Vám za pozornost



TLP: WHITE