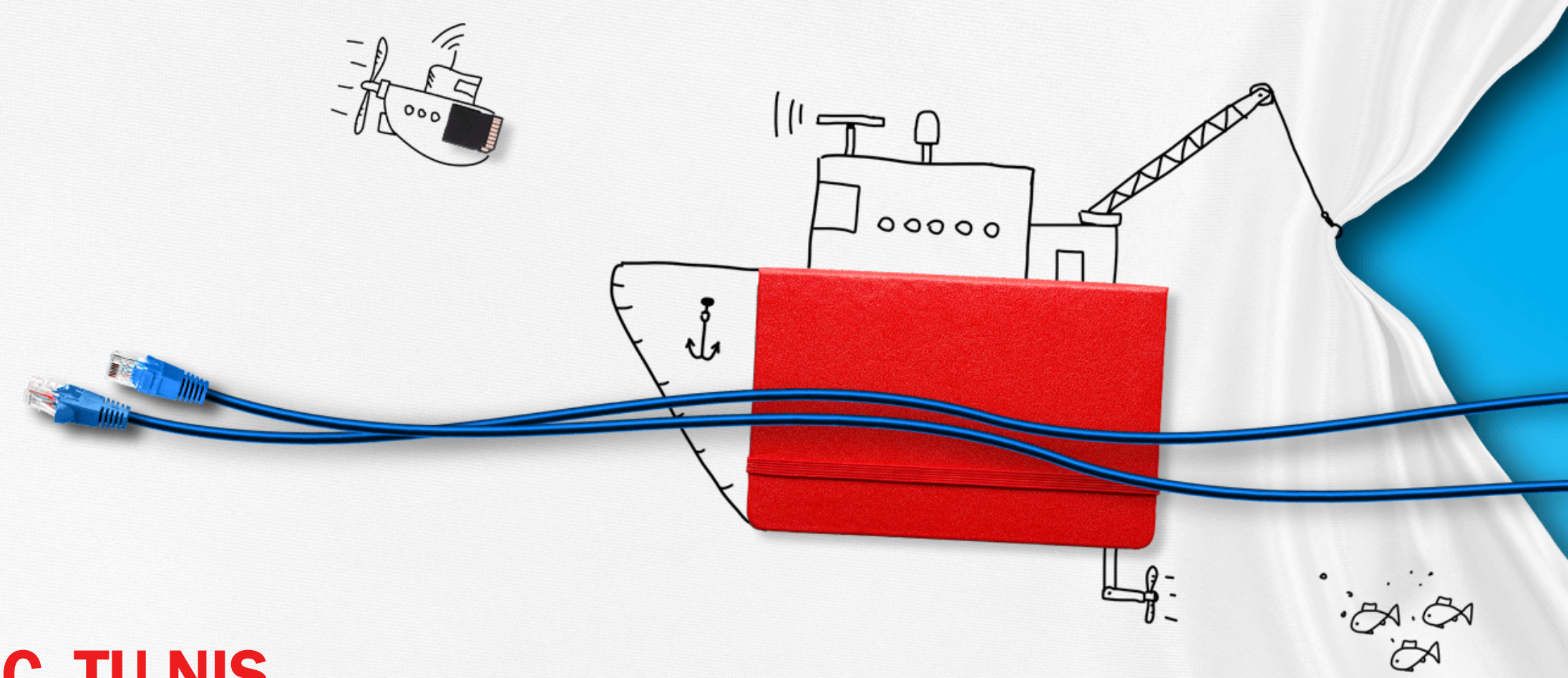
SOITRON



KDE NIC, TU NIS

Lukáš Termer, Security/Presales Architect, Fortinet FCP

PAMATUJETE GDPR?

VVV - Vystrašit, vyfakturovat, vypadnout.

- Pro české firmy jsou rozhodující konkrétní povinnosti definované v ZoKB a navazujících vyhláškách.
- NIS2 není zákon, podle kterého vás bude auditovat NÚKIB.
- Nepodléhejte panice, NIS2 je evropská směrnice.
- V ČR se musíme řídit českým zákonem o kybernetické bezpečnosti (ZoKB) a českými vyhláškami.

NIS2 – EVROPSKÝ SMĚR

- NIS2 říká čeho chce EU dosáhnout, ZoKB říká jak to bude fungovat v ČR.
- Audit, kontroly i sankce budou vycházet z českého ZoKB a navazujících vyhlášek.
- NIS2 je společný evropský základ, ale každá země si implementaci upravila podle svého prostředí.
- Nestačí mít NIS2-ready produkt, důležité je, jestli vám pomůže splnit konkrétní požadavky ZoKB a **hlavně, zda dává smysl i koncepčně.**

NEJSME JEN DODAVATEL TECHNOLOGIÍ

- Pomáháme zákazníkům propojit legislativní požadavky s reálnými bezpečnostními opatřeními a pochopit celý proces.
- Ve spolupráci s prověřenými partnery pomáháme zákazníkům v oblastech:
  - analýza rizik,
  - BCM / BCP,
  - DR plány,
  - gap analýzy,
  - auditní připravenost
  - governance a procesy a další.
- Věříme v transparentní rozdělení rolí mezi auditní a implementační částí projektu.

Technologie samy o sobě compliance nezajistí. Ale správně navržená bezpečnostní platforma výrazně usnadní splnění požadavků ZoKB a zároveň zvýší reálnou bezpečnost.

Technologie Fortinet vnímáme jako jeden z klíčových nástrojů pro budování centralizované viditelnosti, řízení a reakce na bezpečnostní události.

VYBRANÁ SHODA OBLASTÍ S TECHNOLOGIEMI FORTINET

Bezpečnost komunikačních sítí	Segmentace sítě, řízení a kontrola komunikace mezi segmenty, ochrana perimetru i vnitřní sítě	FortiGate, FortiSwitch, FortiAP, FortiNAC
Řízení přístupových oprávnění a identit	Centralizované řízení identit a přístupů, vícefaktorové ověřování, minimální oprávnění	FortiAuthenticator, FortiToken, FortiClient (ZTNA, VPN), FortiPAM
Detekce kybernetických bezpečnostních událostí	Centralizovaný sběr logů, korelace událostí, detekce hrozeb v síťovém provozu i na koncových stanicích, včasné varování	FortiSIEM/FortiAnalyzer, FortiGate, FortiEDR, FortiNDR, FortiDeceptor
Ochrana elektronické pošty a koncových uživatelů	Ochrana e-mailové komunikace proti phishingu, malwaru a spamům, ochrana před útoky na uživatele, zvýšení odolnosti uživatelů	FortiMail, FortiSandbox, FortiEDR, FortiClient, FortiSAT (FortiPhish)

Dříve „nice to have“

Dnes **„must to have“**

VÝBĚR TECHNOLOGIÍ

- FortiDeceptor
  - Nastraží a provozuje „pasti“ (decoy), které napodobují reálné systémy a aplikace, aby na sebe přitahovaly útočníky místo produkční infrastruktury.
- FortiPAM
  - Centrálně spravuje privilegované účty a přístupy (např. admin účty/dodavatelů) a zaznamenává jejich činnost, aby se zabránilo zneužití a usnadnil audit.
- FortiNDR
  - Analyzuje síťový provoz aby odhalil skryté a pokročilé útoky, které obchází klasická zabezpečení.
- voidSOC
  - Bezpečnostní dohledové centrum SOC jako služba - 24/7 monitoring, detekce a reakce na incidenty napříč infrastrukturou zákazníka.