Ochrana citlivých dat a monitoring vnitřního provozu (DLP)

31.5.2024

Security Talk Ostrava

safetica

Michal Novotný

Channel Account Manager

safetica

- Česká společnost
- Od roku 2011
- 90+ bezpečnostních expertů
- 1M+ chráněných zařízení
- V 120+ zemích světa
- Technologické aliance

Kdo jsme

FORTINET Fabric-Ready

Microsoft

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

LOGmanager

RED HERRING EUROPE WINNER 100

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

Info Security Products Guide 2019 GLOBAL EXCELLENCE BRONZE ★★★★★

safetica

- Interní bezpečnost dat = **ochrana proti vnitřním hrozbám**
- **Lidský faktor** je podle dostupných informací zodpovědný za více než 80% případů úniků dat
- Hrozba = člověk, **běžný uživatel**
- Nejedná se o hackera (externí hrozba), ani o **IT profesionála**
- Základní rozdělení: **ZÁMĚR** / ÚMYSL x **OMYL** / NEZNALOST

Co nebo kdo je hrozba?

safetica

- **Soukromý sektor zdravotnictví, reprodukční klinika:**
  - Při implementaci řešení zkopírování velkého objemu citlivých zdravotnických dat na USB disk, pokus o fyzické vynesení z organizace, dohledaná komunikace s konkurencí, ukončení pracovního poměru
  - Citlivá data: osobní, speciální kategorie zdravotnických citlivých dat
- **Výrobní sektor automotive:**
  - Při náboru konstruktérů získání konstrukčních dat od několika předchozích zaměstnavatelů
  - Dojem, že vytvořená data jsou majetkem jednotlivce, nikoli společnosti
  - Regulace TISAX (Trusted Information Security Assessment Exchange), nutnost nasazení DLP řešení, citlivá data: konstrukční, výkresy, pod NDA, práce s nimi podléhá certifikaci

Příklady z praxe

safetica

- **Další:**
  - **Odesílání interních dat společnosti bývalému zaměstnanci emailem**
  - **Záloha firemních dat na soukromý cloud, střední management**
  - **Zkopírování seznamu zákazníků leasingové společnosti za účelem poskytnutí konkurenci**
  - **Nahrání interních finančních dat do veřejného prostoru včetně detailů o odměňování managementu**

Příklady z praxe

Vnitřní hrozby jsou na vzestupu

45 %

zaměstnanců si při odchodu ze zaměstnání s sebou bere firemní data[1]

88 %

společností nedokáže důsledně odhalit vnitřní hrozby[2]

68 %

úniků dat trvá měsíce, než se odhalí[1]

2 měsíce

v průměru trvá řešení incidentu způsobeného vnitřní hrozbou[3]

$3,86 milionu

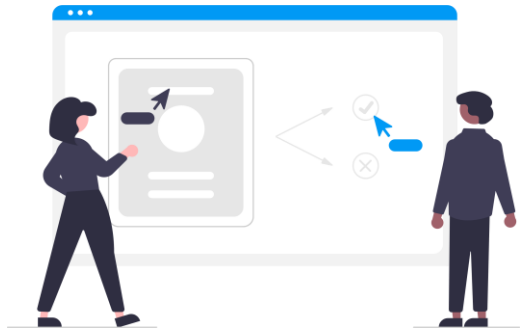
průměrně zaplatí organizace postižené únikem dat[3]

[1] *Verizon 2021 Data Breach Investigations Report*
[2] *Bitglass 2019 Insider Threat Report*
[3] *2020 Cost of Data Breach Report, Ponemon Institute*

Klíčové trendy

Rostoucí význam dat a lidí jako motoru pro moderní firmy

Rostoucí důraz na ochranu osobních údajů a dodržování předpisů



Práce na dálku a přesun do digitálního pracovního prostředí vyžaduje vyšší kontrolu nad daty

Rostoucí množství a důraz na regulace

- **NIS 2**
  - Nová směrnice EU o kybernetické bezpečnosti
- **TISAX**
  - Trusted Information Security Assessment Exchange
  - Standard pro automotive sektor a spolupracující společnosti

safetica

safetica

- **Uveřejněna** v rámci EU 27.12.2022
- **Platnost** v rámci EU od 16.1.2023
- Do českého právního řádu bude implementována prostřednictvím nového **zákona o kybernetické bezpečnosti**
- Předpoklad **přijetí** nového **ZoKB** do 16.10.2024

NIS 2

safetica

TLP: CLEAR

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

VÝZKUM

Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

Subjekty shromažďující a udržující přesnou a úplnou registraci názvu domén.

verze 1.0, platná ke dni 16.08.2022

Koho se týká – Poskytovatel regulované služby

safetica

- Registrace na portálu **NÚKIB**u (ne všichni, samoidentifikace nebo zahájení řízení u velmi důležitých organizací pro stát)
- Hlásit **kontaktní a další údaje** (návrh NÚKIB)
- Stanovit rozsah řízení kybernetické bezpečnosti (**klasifikace aktiv a rizik**)
- **Zavádět** bezpečnostní organizační opatření, konkrétně pak například **systém řízení bezpečnosti informací**
- **Hlásit** kybernetické bezpečnostní incidenty
- Informovat o **incidentech** a hrozbách zákazníky
- **Další**

Povinnosti

safetica

- **Organizační opatření:**
  - **Systém řízení bezpečnosti informací**
  - Bezpečnostní role
  - **Řízení bezpečnostní politiky a bezpečnostní dokumentace**
  - **Řízení aktiv**
  - **Řízení rizik**
  - **Bezpečnost lidských zdrojů**
  - Řízení přístupu
  - Zvládání kybernetických bezpečnostních událostí a incidentů
  - Audit kybernetické bezpečnosti
  - A další

Seznam bezpečnostních opatření pro poskytovatele regulované služby v režimu vyšších povinností

Zdroje a informace

- **NÚKIB**: https://osveta.nukib.cz/course/view.php?id=145
- Blog Safetica: **NIS2: Rozsah, účel a jaké změny očekávat**
- **Materiál** popisující průnik směrnice a technologie Safetica DLP

safetica

safetica

NIS 2

DOPAD DO AKTUALIZACE ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A VYHLÁŠKY O BEZPEČNOSTNÍCH OPATŘENÍCH POSKYTOVATELE REGULOVANÉ SLUŽBY V REŽIMU VYŠŠÍCH POVINNOSTÍ

17.08.2023

safetica

- **T**rusted **I**nformation **S**ecurity **A**ssessment E**x**change (důvěryhodné hodnocení informační bezpečnosti)
- Je postaven na klíčových prvcích normy **ISO/IEC 27001**
- Zavádí asociace ENX (**European Network Exchange**) pro evropský automobilový průmysl (**výrobci i dodavatelé**)
- Ať už se vaše spolupráce týká **finančních služeb, eventů, fotografování, marketingu, práce s dokumenty či výroby/dodávání do automobilového průmyslu**, bude po vás certifikace TISAX® požadována

TISAX

safetica

- Velké **rozdíly v kvalitě** u normy ISO/IEC 27001 (jednotlivé firmy, auditní firmy, země)
- Nad rámec této normy stanovuje **doplňující specifikace** zohledňující prostředí automobilového průmyslu
- Otázka bezpečnosti informací patří mezi **nejdůležitější faktory konkurenceschopnosti**

Proč

safetica

- **Úroveň 1: "Normální"** úroveň zabezpečení. Organizace musí pouze vyplnit dotazník pro sebehodnocení. Tato úroveň je při obchodování většinou irelevantní a často se používá pouze interně.
- **Úroveň 2: "Vysoká"** úroveň zabezpečení. Schválený poskytovatel auditu naváže na sebehodnocení telefonickou kontrolou věrohodnosti. To znamená rozhovor na dálku založený na dokumentech a přezkoumání poskytnutých důkazů.
- **Úroveň 3: "Velmi vysoká"** úroveň zabezpečení. Kontrolu, rozhovory a posouzení ISMS (systému řízení bezpečnosti informací) provádí schválený poskytovatel auditu, který organizaci fyzicky navštíví. Pokud je organizace rozdělená do více lokací, může auditor navštívit každou z nich.

Tiers - Úrovně

Zdroje a informace

- **Internet, auditní firmy**
- Blog Safetica: **TISAX: Rozsah, účel a způsoby plnění požadavků**
- **Materiál** popisující průnik standardu a technologie Safetica DLP

safetica

Společné rysy NIS 2 a TISAX

- **TISAX** vychází ze standardu ISO 27001
- **NIS 2** obsahuje / vyžaduje stejné věci jako ISO 27001 (některé požadavky)
- Zabývají se mimo jiné / z velké části **systémy řízením bezpečnosti informací** a zabezpečením kyberprostoru organizací (**průnik viz materiály**)
- Za slabá místa často považují **procesy a lidský faktor**

safetica

Jak Safetica pomůže

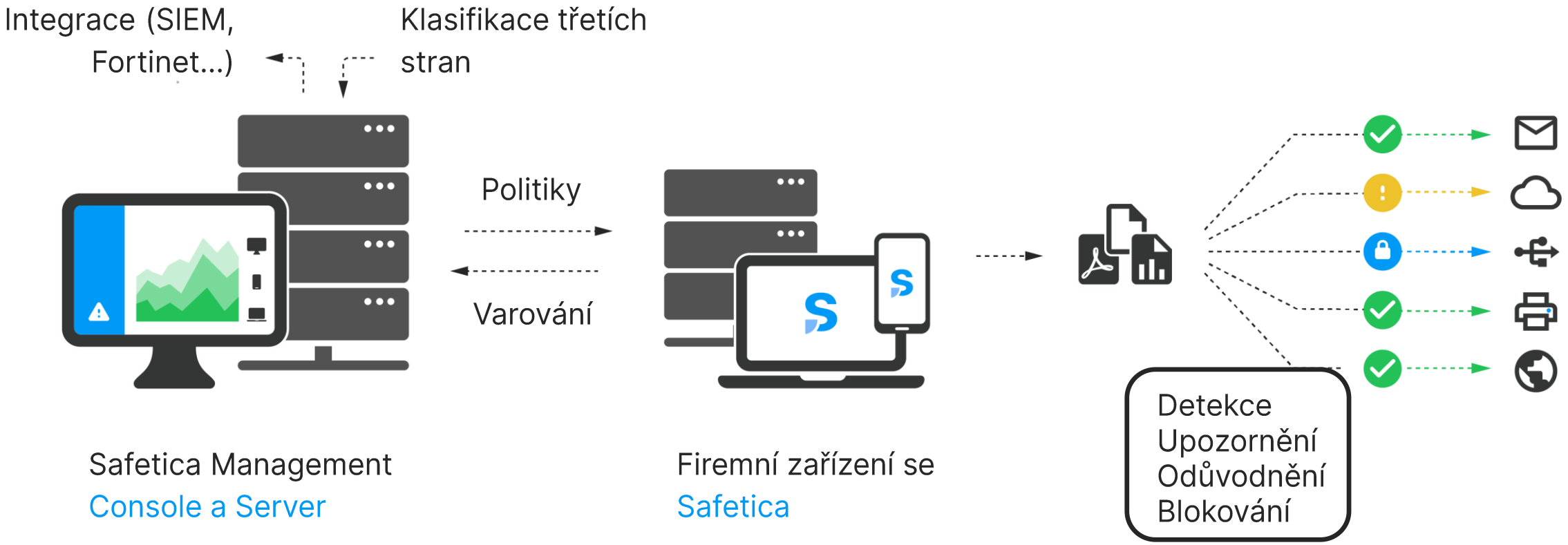
- Zabezpečí **prostředí** proti vnitřním hrozbám
- Dá **přehled** o datech, jejich **tocích a pohybech**, o historii práce s nimi
- Pomáhá splnit **regulace, směrnice, nařízení, standardy, normy**
- Chrání před **lidskou chybou** nejen organizaci, ale i zaměstnance

safetica

safetica

Tři jednoduché kroky

Jak funguje Safetica ONE?

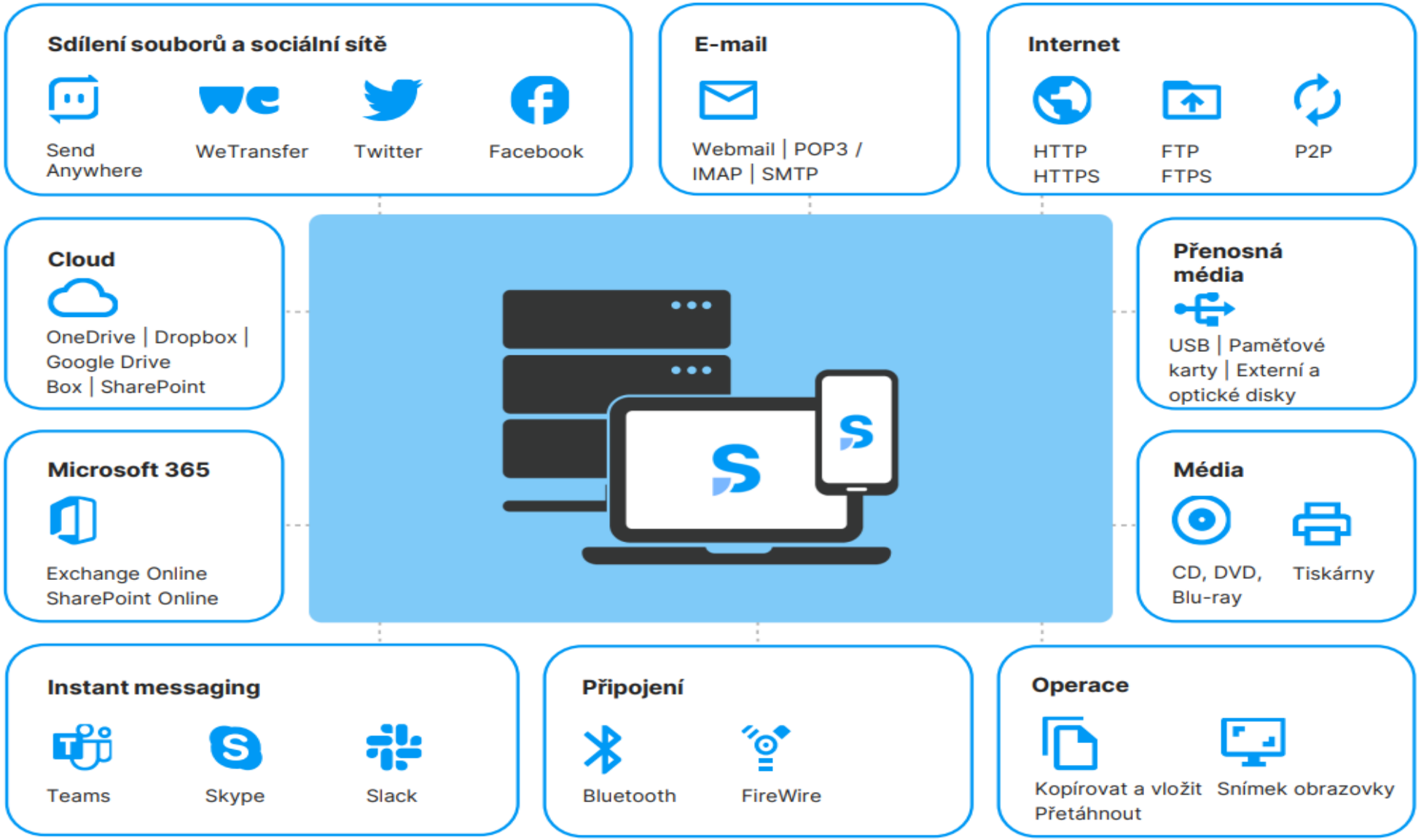


Safetica Management
Console a Server

Firemní zařízení se
Safetica

Pokryté datové kanály

Safetica chrání data napříč různými kanály a platformami. Vaše data budou v bezpečí, ať už se nacházejí kdekoli nebo tečou kamkoli.



Co společnost Safetica odlišuje?

Naše základní kameny

Snadné použití a rychlé nasazení

Pokročilá analýza pracovního prostředí a chování

Dává všem datům jasný kontext

Vysoká flexibilita a použitelnost v různých prostředích

Nízké nároky na hardware koncových zařízení i serverů

Snadná integrace s vaším IT bezpečnostním stackem

Reference

Česká televize

Městská policie Praha

JABLOTRON CREATING ALARMS

tescoma

ROSSMANN
A život je krásnější

BMW invelt
invelt.com

Dr. Müller PHARMA

Generální inspekce bezpečnostních sborů

ALD Automotive

MONETA MONEY BANK

WIKOV

Česká inspekce životního prostředí

KOITO

KŠ LEGAL s.r.o. advokátní kancelář

BAUHAUS

Raiffeisen BANK

CZ For those who know

dpd

ČP SECURITY

211 ZDRAVOTNÍ POJIŠŤOVNA MINISTERSTVA VNITRA ČR

Brož Sedlatý ADVOKÁTNÍ KANCELÁŘ

SKUPINA ČEZ

PPF Banka

ptáček

Česká průmyslová zdravotní pojišťovna

GENERALI ČESKÁ POJIŠŤOVNA

kofola original

TEPLÁRNY BRNO

safetica

Message

- Nebuďte **lhostejní** k vnitřní bezpečnosti vašich dat
- Chtějte **vědět**, co se s vašimi daty děje
- **Rizika** jsou tu pro všechny sektory
- Málokdo dnes ve firmě **nemá** citlivá data

safetica

Děkujeme

Q & A

safetica

+420 777 038 353

michal.novotny@safetica.com