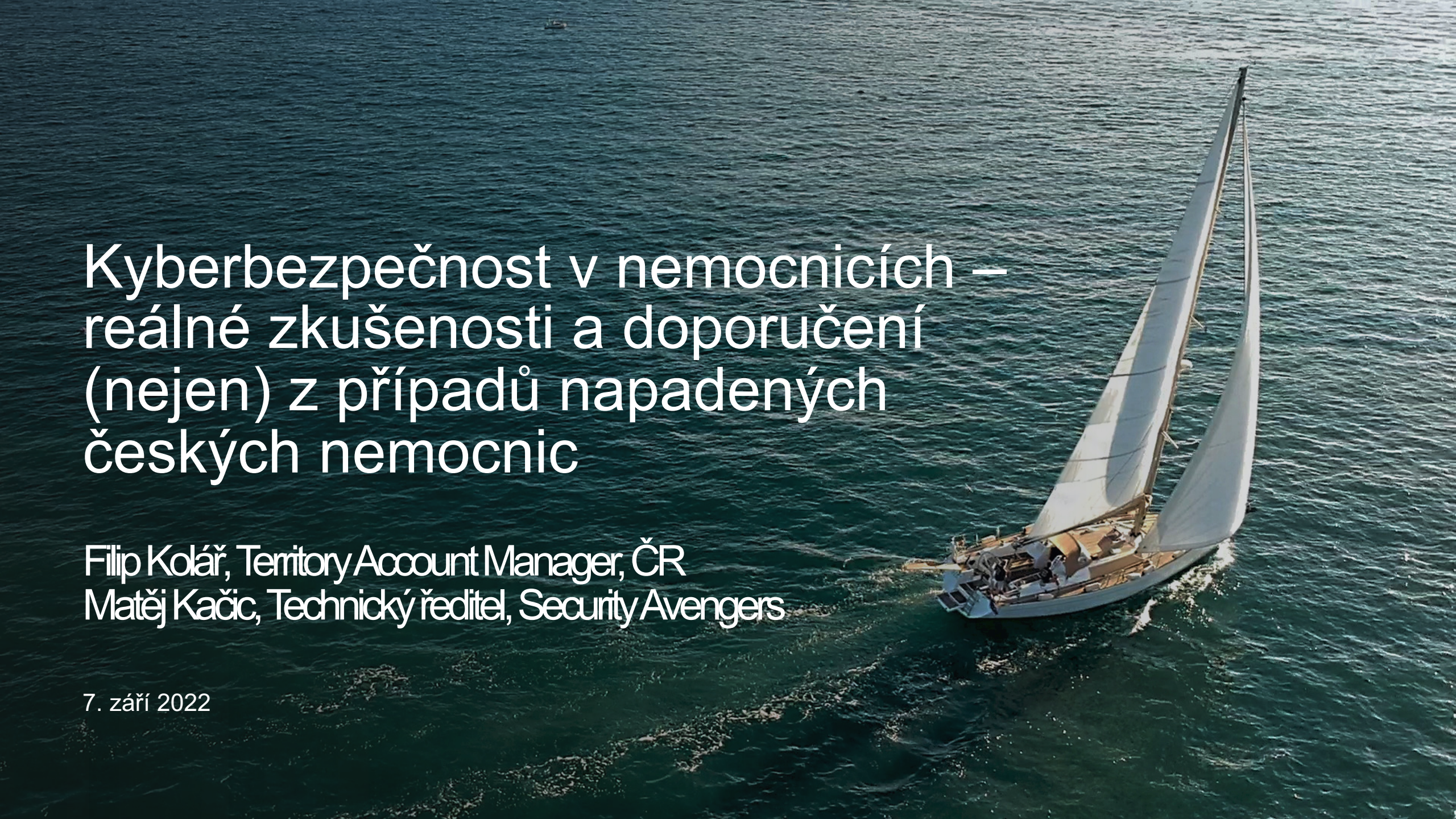
Kyberbezpečnost v nemocnicích – reálné zkušenosti a doporučení (nejen) z případů napadených českých nemocnic

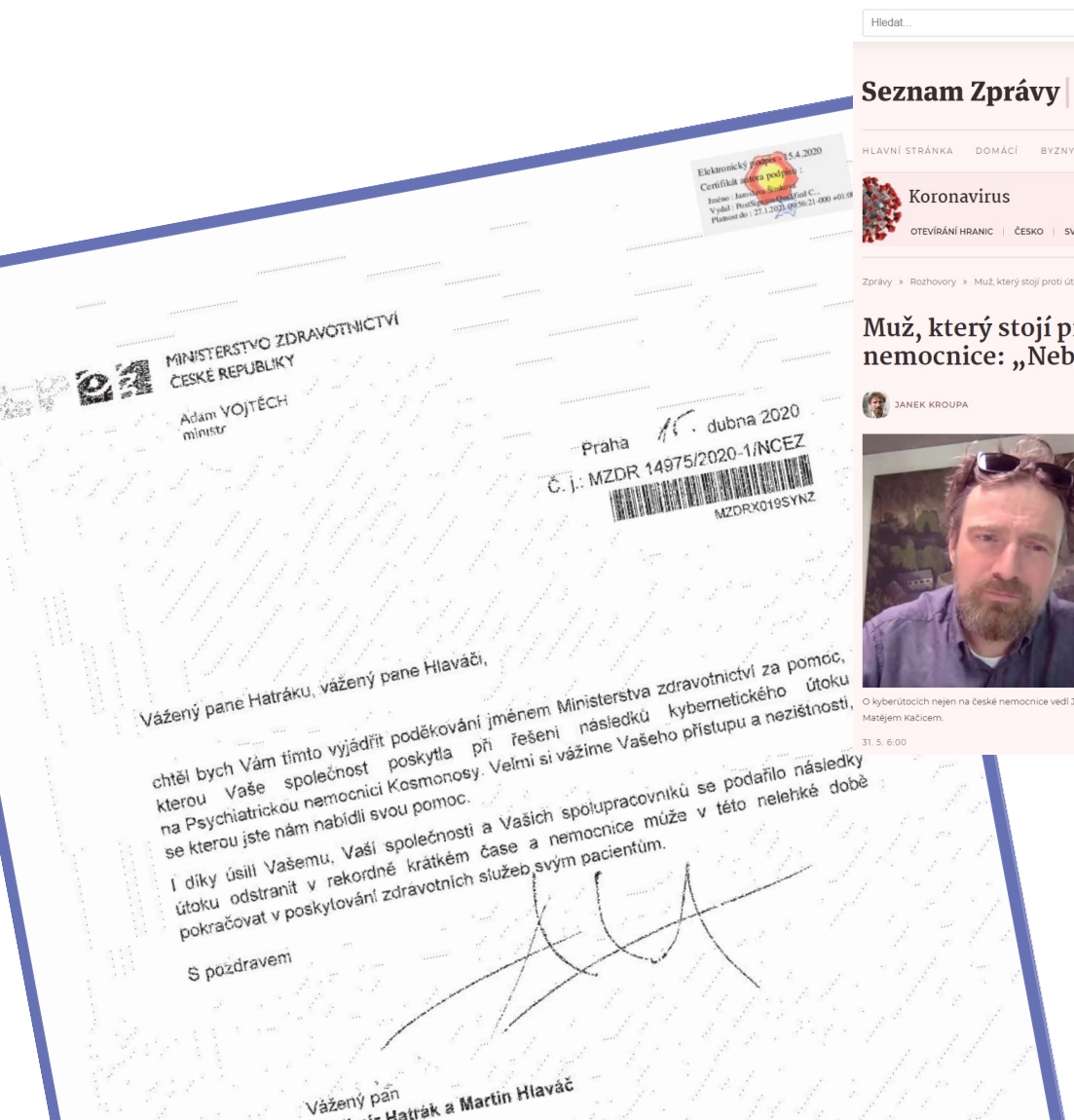
Filip Kolář, Territory Account Manager, ČR
Matěj Kačic, Technický ředitel, Security Avengers

7. září 2022



Obnova napadených nemocnic 2020

https://www.seznamzpravy.cz/clanek/muz-ktery-stoji-proti-utocnikum-na-nemocnice-nebyl-jen-jeden-107958


MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Adam VOJTĚCH
ministr

Praha 17. dubna 2020
Č. j.: MZDR 14975/2020-1/NCEZ
MZDRX019SYNZ

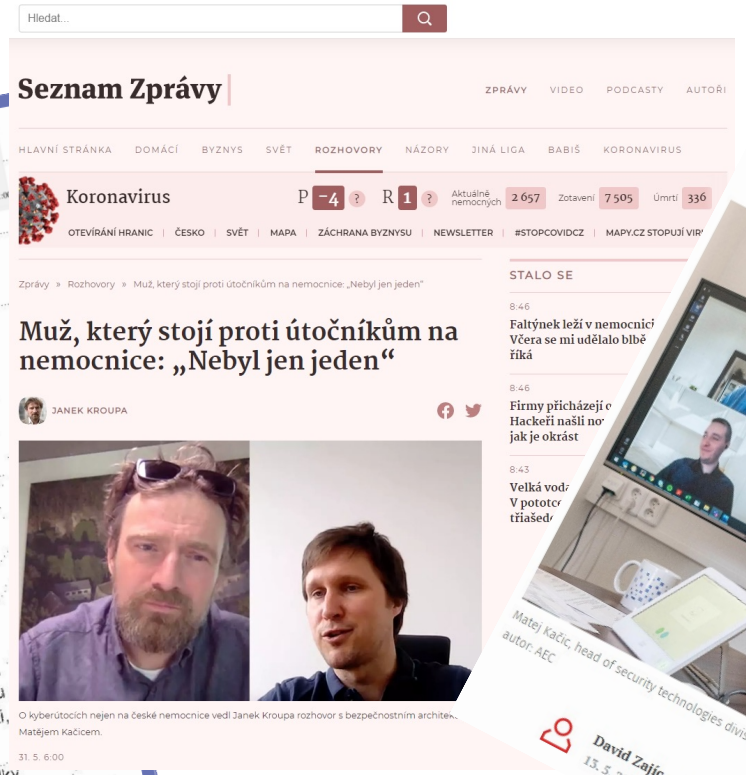
Vážený pane Hatráku, vážený pane Hlaváči,

chtěl bych Vám tímto vyjádřit poděkování jménem Ministerstva zdravotnictví za pomoc, kterou Vaše společnost poskytla při řešení následků kybernetického útoku na Psychiatrickou nemocnici Kosmonosy. Velmi si vážíme Vašeho přístupu a nezištnosti, se kterou jste nám nabídli svou pomoc.

I díky úsilí Vašemu, Vaší společnosti a Vašich spolupracovníků se podařilo následky útoku odstranit v rekordně krátkém čase a nemocnice může v této nelehké době pokračovat v poskytování zdravotních služeb svým pacientům.

S pozdravem

Vážený pan
Hatrák a Martin Hlaváč


Hledat...

Seznam Zprávy

ZPRÁVY VIDEO PODCASTY AUTOŘI

HLAVNÍ STRÁNKA DOMÁCÍ BYZNYS SVĚT ROZHOVORY NÁZORY JINÁ LIGA BABIŠ KORONAVIRUS

Koronavirus P -4 R 1 Aktuálně nemocných 2 657 Zotavení 7 505 Úmrtí 336

OTEVÍRÁNÍ HRANIC | ČESKO | SVĚT | MAPA | ZÁCHRANA BYZNYSU | NEWSLETTER | #STOPCOVIDCZ | MAPY.CZ STOPUJÍ VIR

Zprávy » Rozhovory » Muž, který stojí proti útočníkům na nemocnice: „Nebyl jen jeden"

Muž, který stojí proti útočníkům na nemocnice: „Nebyl jen jeden"

JANEK KROUPA

STALO SE

8:46
Faltýnek leží v nemocnici
Včera se mi udělalo blbě
říká

8:46
Firmy přicházejí o
Hackeři našli no
jak je okrást

8:43
Velká voda
V pototo
tříašed

O kyberútocích nejen na české nemocnice vedl Janek Kroupa rozhovor s bezpečnostním archite
Matějem Kačicem.

31. 5. 6:00


HOSPODÁŘSKÉ NOVINY

KORONAVIRUS BYZNYS ZPRÁVY NÁZORY TECH VÍKEND PROČ NE?! PODCASTY ANDĚLÉ HN EVENTS

Nemocnice ochromily kybernetické útoky

Matej Kačic, head of security technologies division, AEC

David Zajíc, redaktor
13. 5. 2020 / 00:00 / 9 minut čtení

https://ictrevue.ihned.cz/c3-66768270-0ICT00_d-66768270-nemocnice-ochromily-kyberneticke-utoky

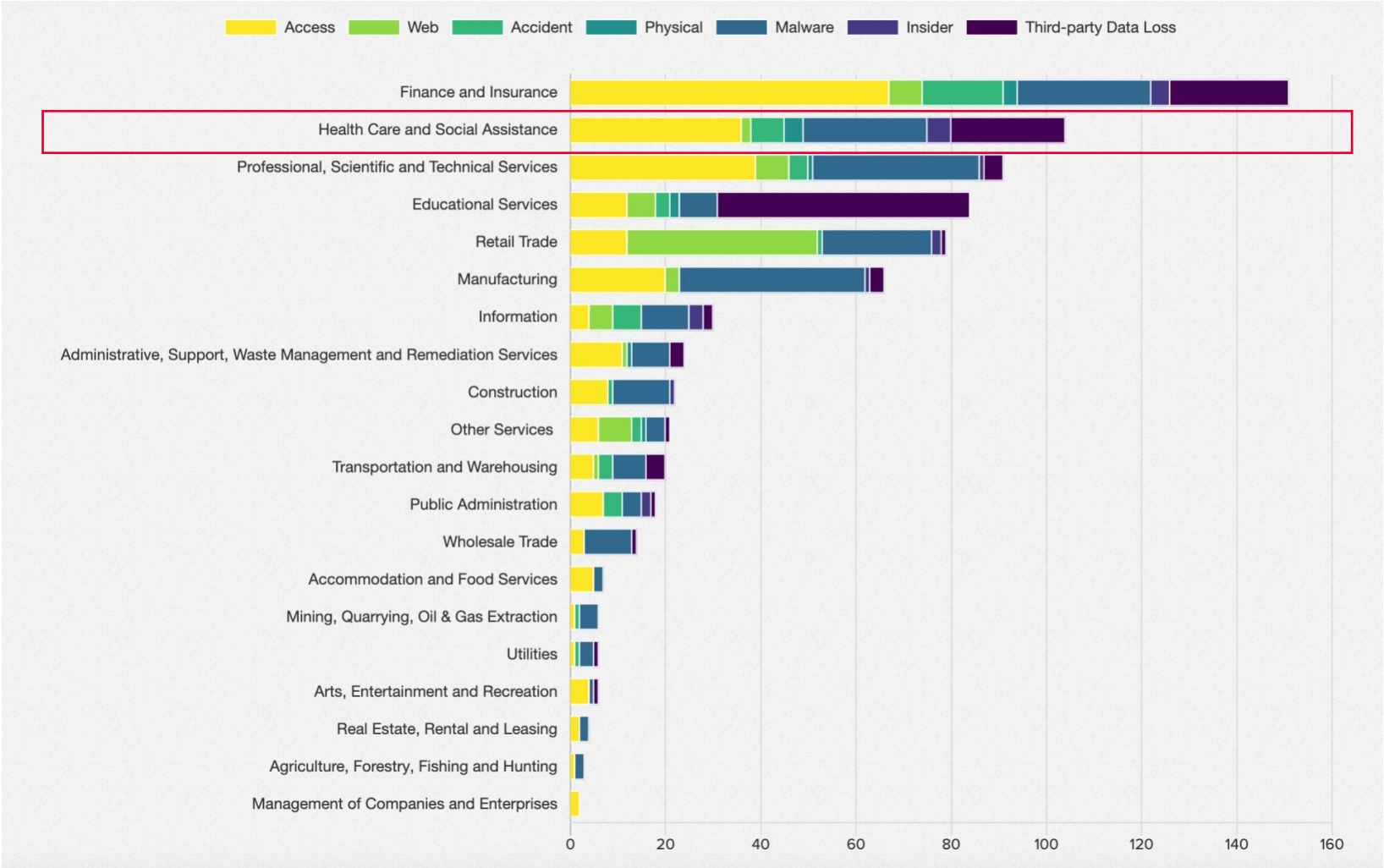
AGENDA

- Současné techniky útočníků
- Jak pomůže F5
- Anatomie útoků
- Doporučená bezpečnostní architektura

Security Avengers

Současné techniky útočníků

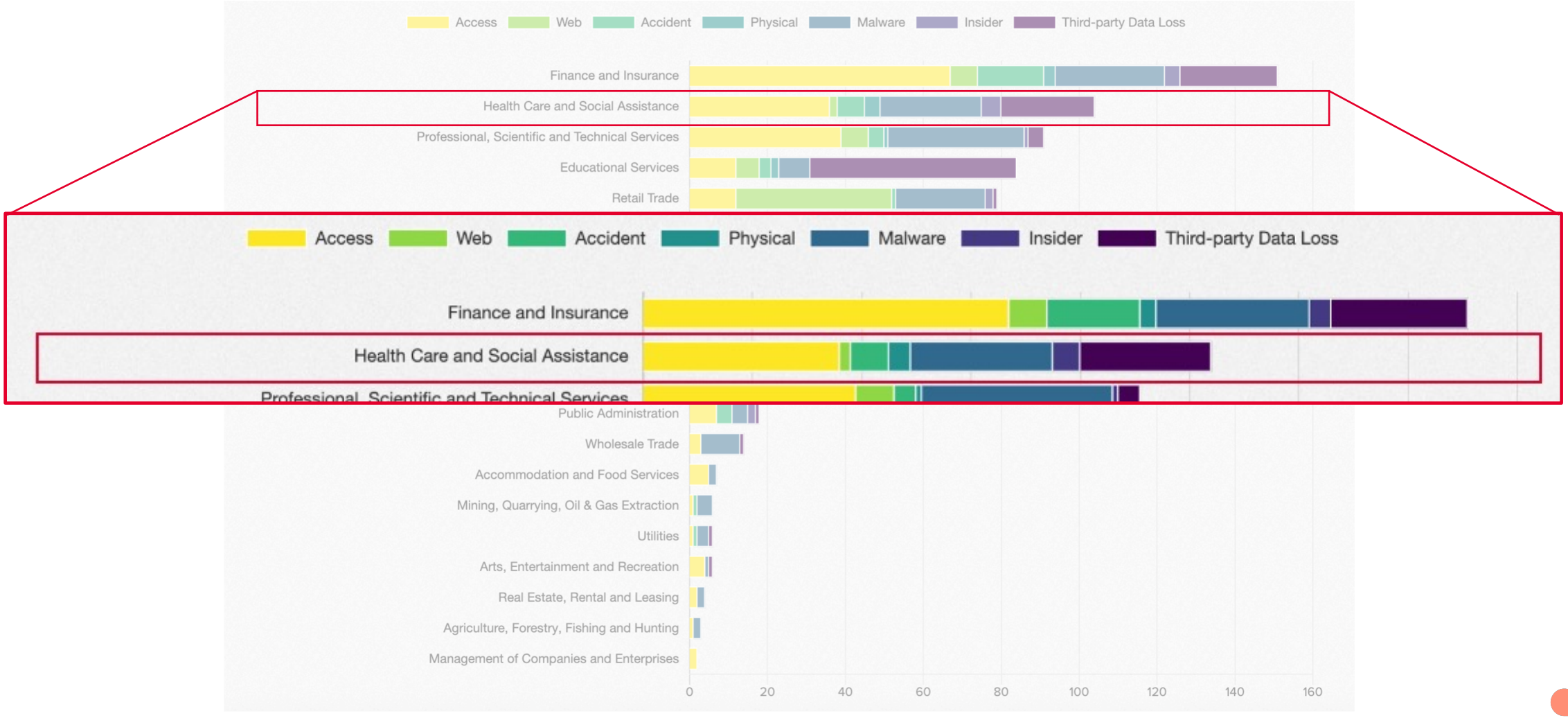
Zdravotnictví patří mezi druhým ”nejoblíbenější” odvětví mezi útočníky



https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-in-expectation-of-exfiltration

Security Avengers

Útoky jsou vedené pomocí přístupů, malwaru, služeb 3. stran a webových služeb

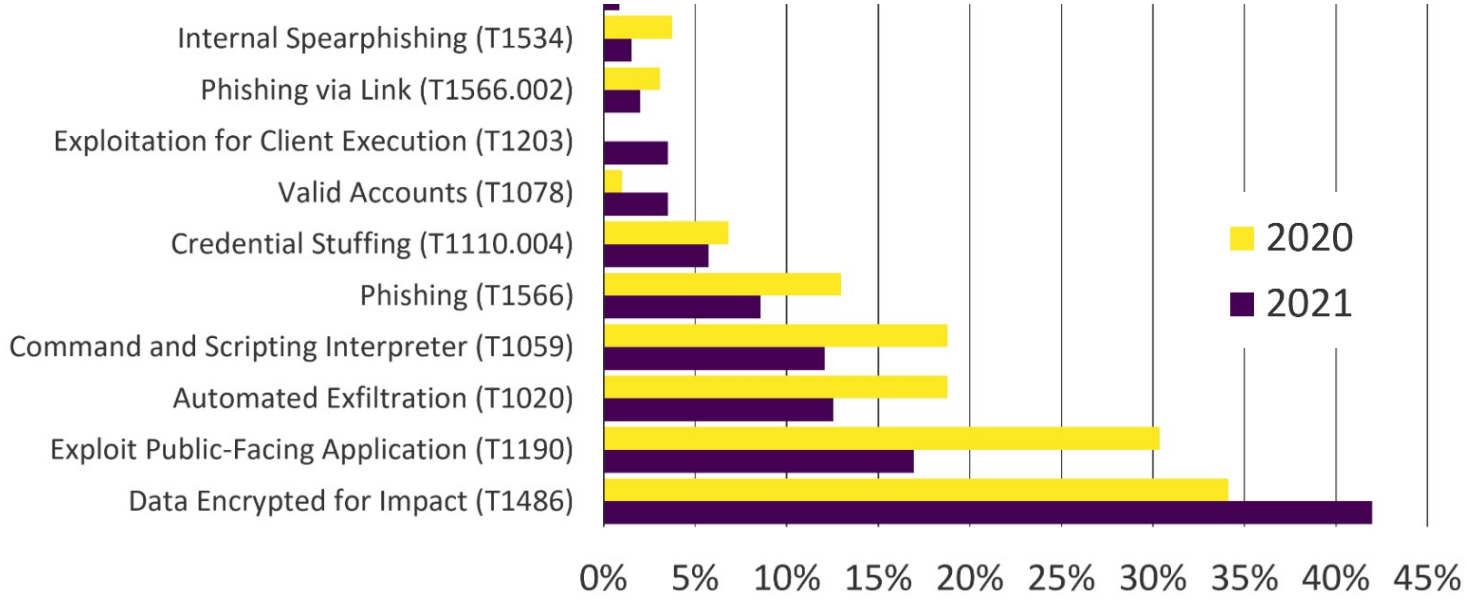


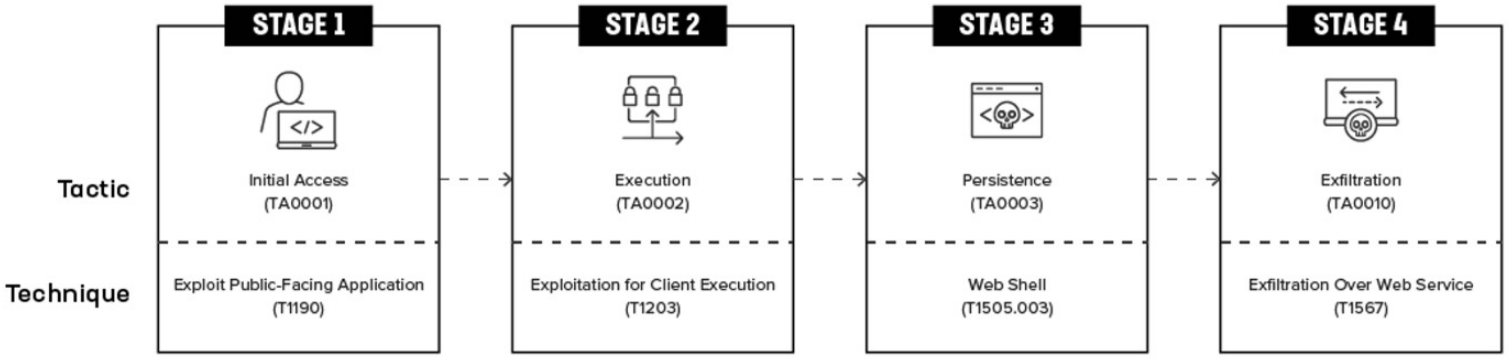
https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-in-expectation-of-exfiltration

Security Avengers

Útočník většinou kombinuje různé vektory

F5 LABS APPLICATION THREAT INTELLIGENCE





Security Avengers

zdroj NÚKIB

Útoky na české nemocnice (2020) – vektory útoku identické se závěry F5 SIRT

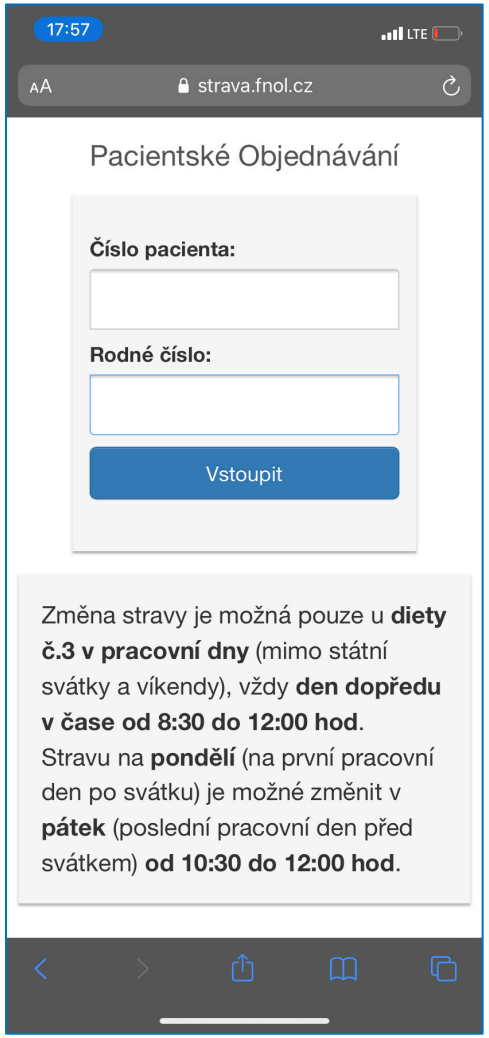
Ransomware – vektory útoku a prevence

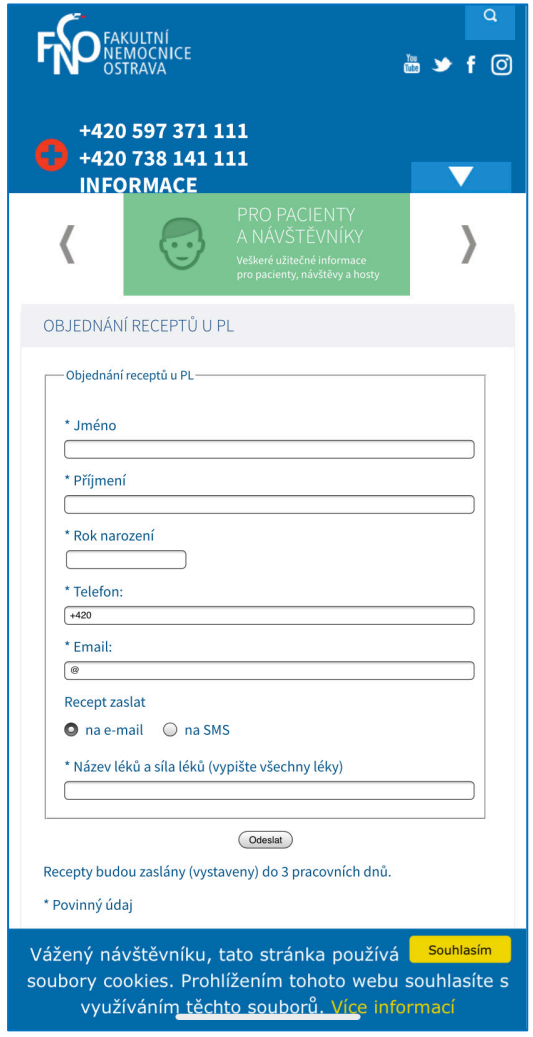
- Vektory útoku
  - Phishing/spear-phishing
  - Bruteforce na otevřené služby
  - Zneužití zranitelného zařízení či služby
  - Zneužití odcizených přihlašovacích údajů
  - Kompromitace skrze poskytovatele služeb
- Prevence
  - Zálohy (i offline)
  - Segmentace sítě
  - Aktualizace
  - Otevřené služby – ponechat jen ty nezbytné
  - Uživatelé
  - Hesla
  - Uživatelské účty
  - Emaily a přílohy
  - Logy

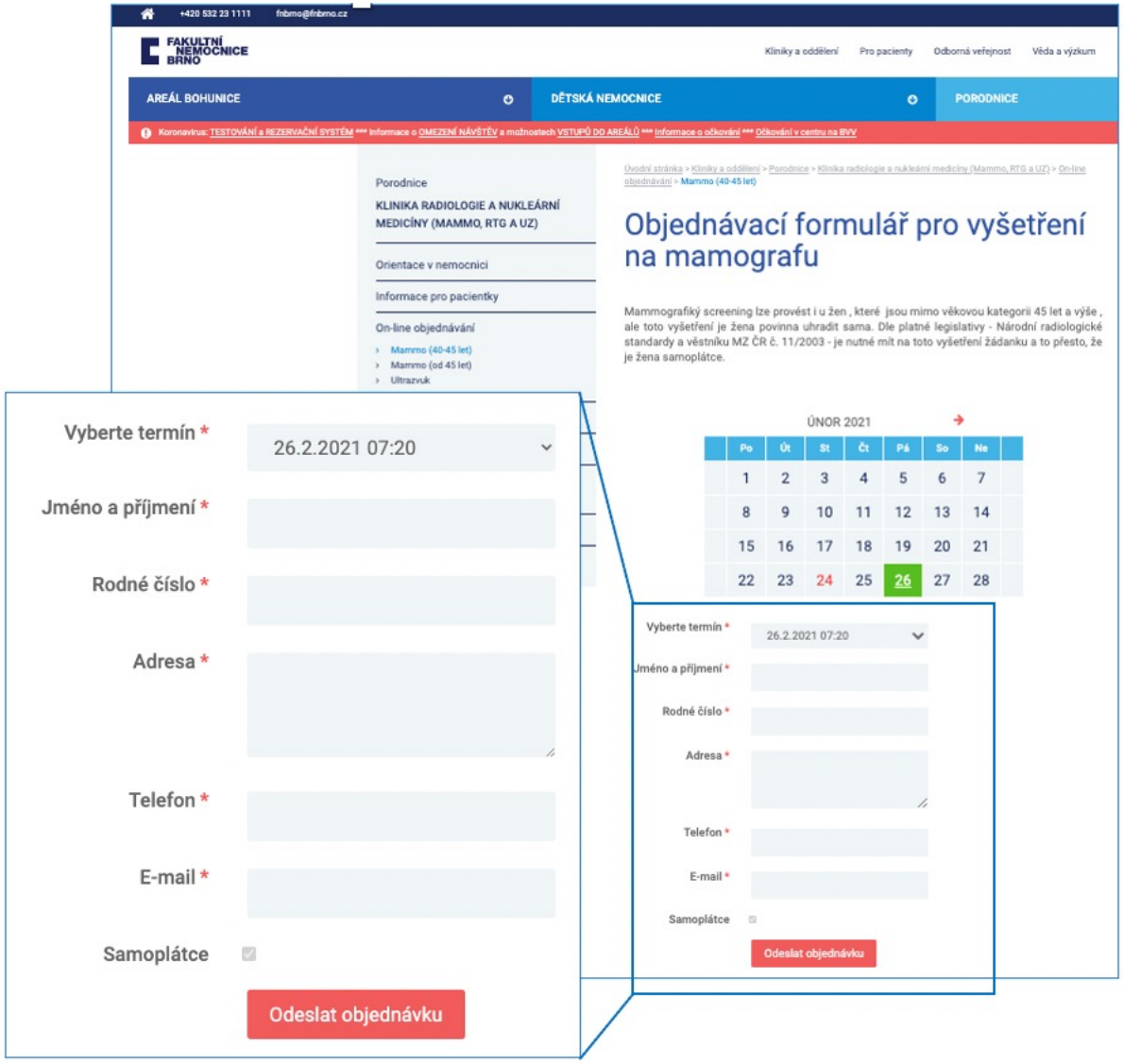
+ reakce - krizový plán, kdyby se to stalo

Více viz podpůrný materiál: https://www.nukib.cz/cs/infoservis/aktuality/1662-jak-se-branit-utoku-ransomwarem/

S digitalizací nemocnic se zvyšuje počet webových aplikací publikovaných do internetu

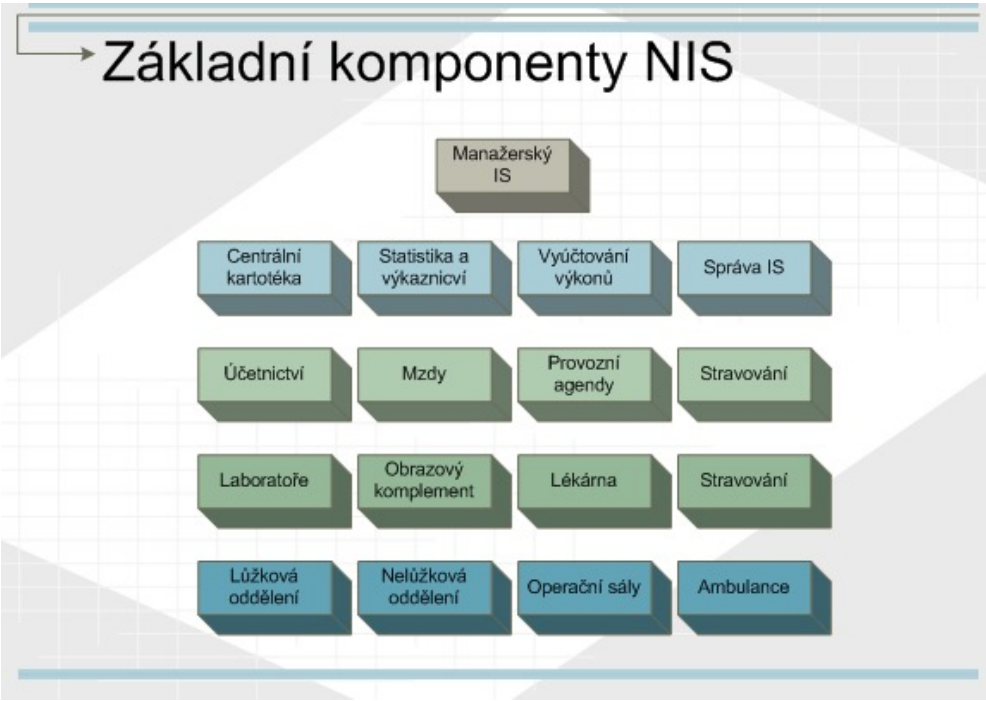






Webové NIS je potřeba chránit web aplikačním firewallem

NIS nemusí být publikovaný do internetu, aby došlo k exfiltraci dat.



Kritické informace o pacientech v klinické části NIS:

Elektronická zdravotní dokumentace je obdobou dokumentace papírové, zahrnuje anamnestické údaje pacienta, nálezy a zprávy z provedených vyšetření, závěry konzilií, výsledky laboratorních vyšetření a vyšetření zobrazovacími metodami, popis průběhu ošetření (dekurs), epikrízy (zpravidla týdenní souhrny zdravotního stavu pacienta, prognózy dalšího vývoje a plánovaný postup léčby), diagnózy, klasifikaci příčin hospitalizace a případných komplikací a komorbidit v klasifikačním systému MKN-10, operační protokoly, medikaci, přijímací, překladové a propouštěcí zprávy a další údaje.

Ransomware je o riziku zašifrování, odcizení a zveřejnění dat, nebo narušení jejich integrity.

Jak pomůže F5

Jak může pomoct F5?

- **Vysoká dostupnost a rychlé webové služby.**
- **Terminace a inspekce SSL**
- **Ochrana kritických aplikací** v internetu a interní síti.
- **Eliminace nálezů z penetračních testů** v aplikacích.
- **Autentizační brána** / SSO / Zero Trust.

- **Shoda ZoKB** §19, §25, §26, §27.
- **Eliminace TOP bezpečnostních problémů**.
- **Visibilita** a schopnost předvídat útok.
- **Nezávislost na** vývojovém týmu a **verzích SW třetích stran**.

Security Avengers

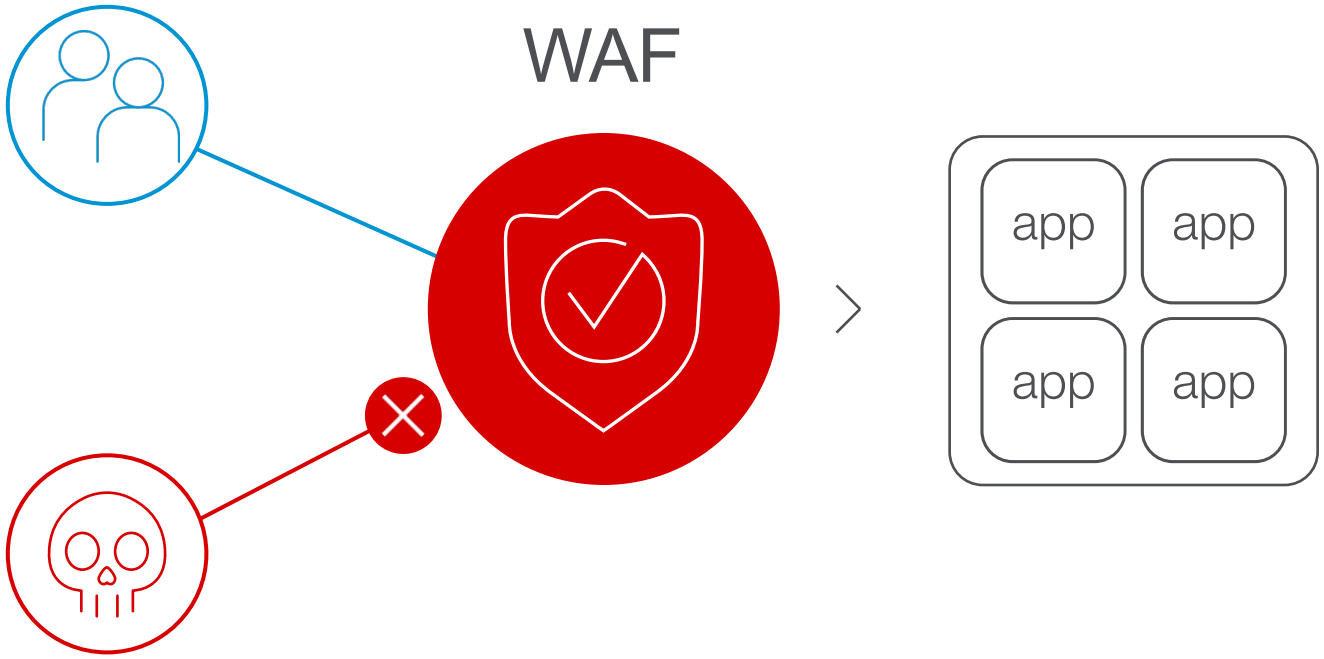
Zákazníci v ČR a na Slovensku

- Finance – Banky, nebankovní instituce, platební brány
- Komerční sektor – Sázkové kanceláře, utility, …
- Operátoři – Telco, ISP, MSP
- Státní správa a podniky - Ministerstva, kraje, velké státní podniky

https://customers.microsoft.com/en-gb/story/1452435703603766752-f5-partner-professional-services-microsoft-azure-commercial-marketplace

Vysoká dostupnost
Terminace a inspekce SSL
Aplikační ochrana

WAF není FW :-)

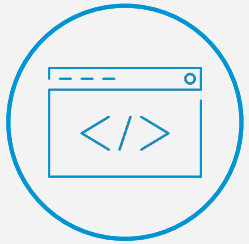


- Zranitelnosti
- Aktivní útoky
- Compliance

Tradiční WAF

OWASP Top 10

SSL/TLS Inspection

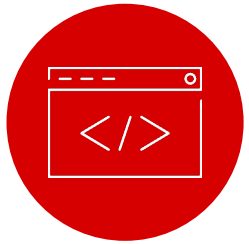


Scripting

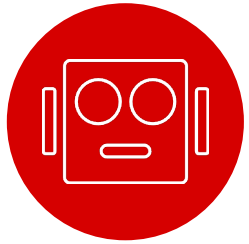
Pokročilá WAF

OWASP Top 10

SSL/TLS Inspection

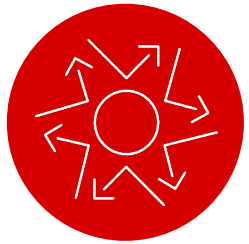


Scripting



Proactive Bot Defense

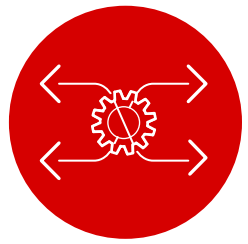
Credential Protection



App-Layer DoS Protection

Threat Campaigns

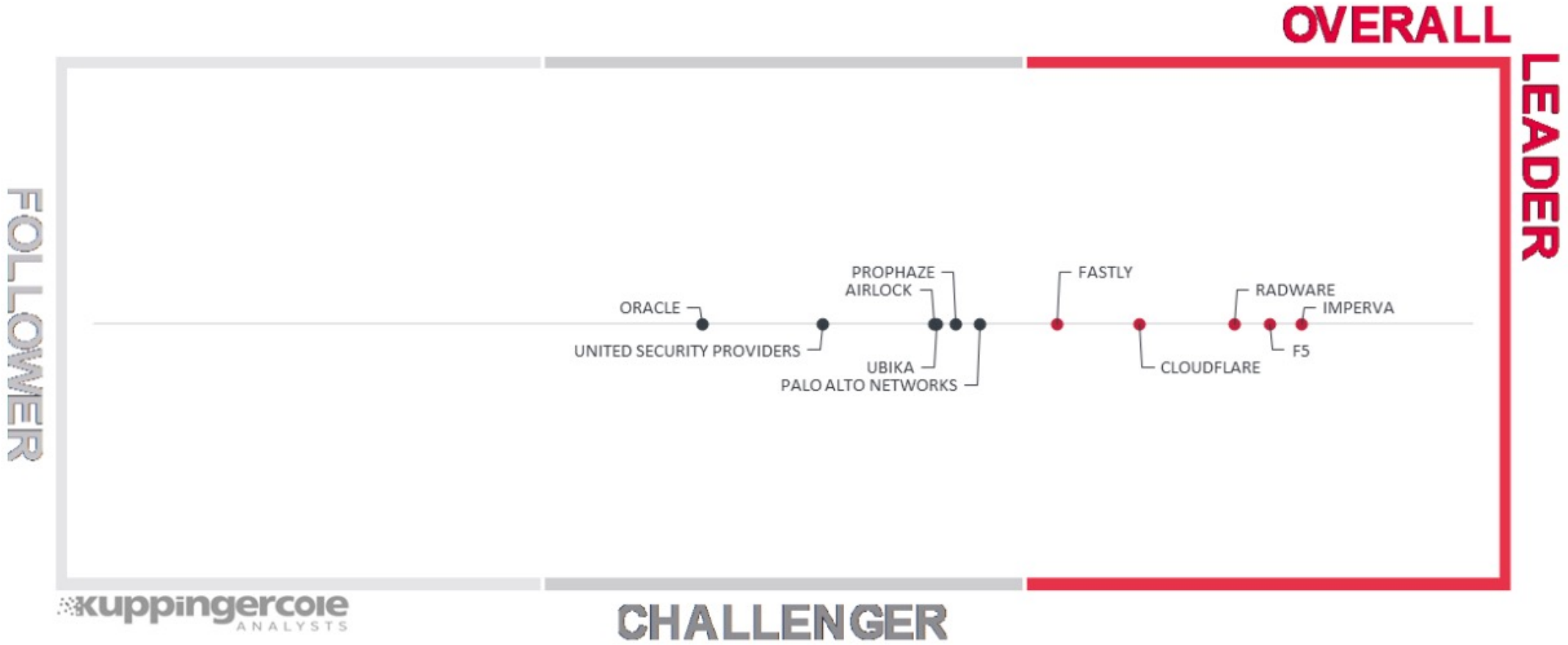
Credential Stuffing



API Security

Kuppingercole: F5 je TOP3 WAF na trhu

Web Application Firewalls 2022

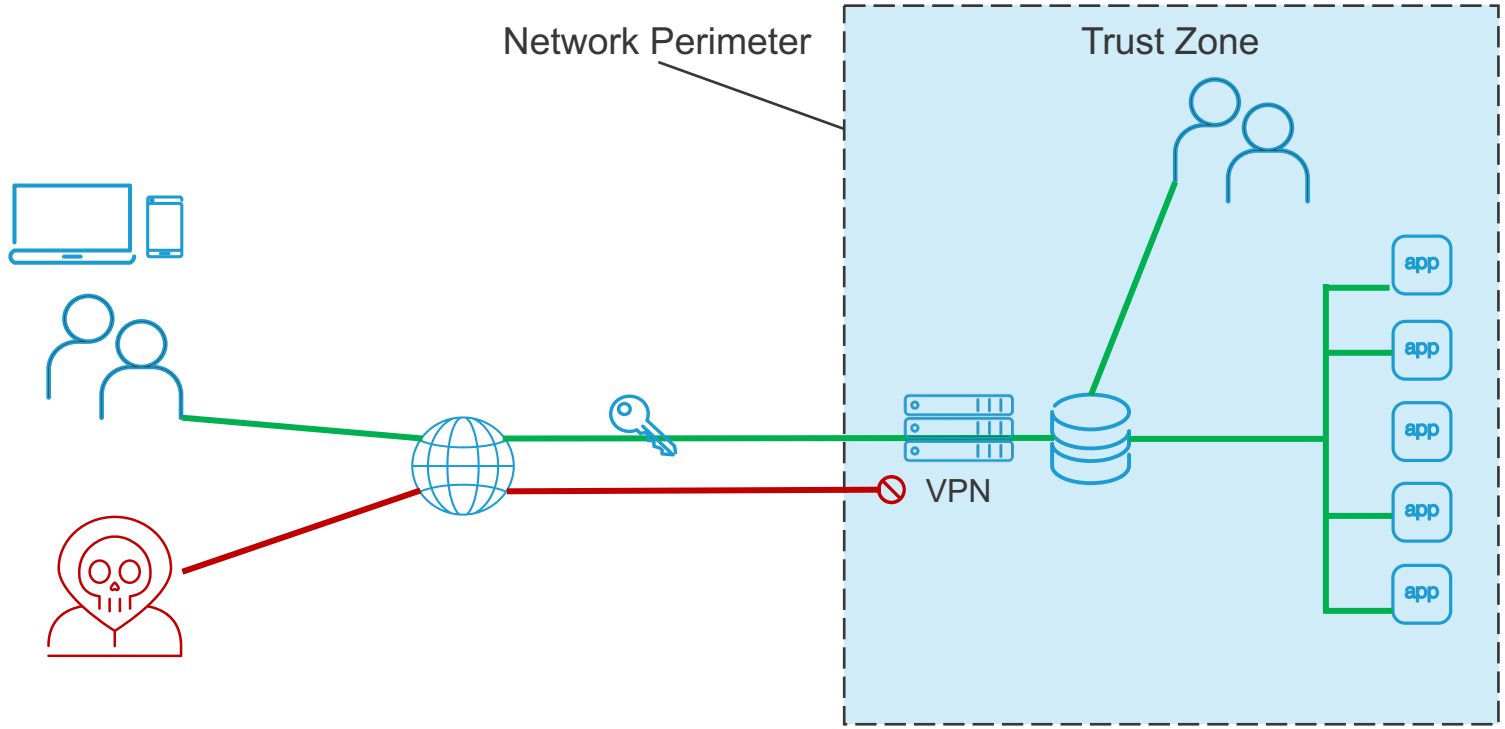


https://www.kuppingercole.com/reprints/4978b7e8ad8937ca27ae09eef19740a1

Vzdálený přístup k aplikacím
Autentizační brána / Zero Trust

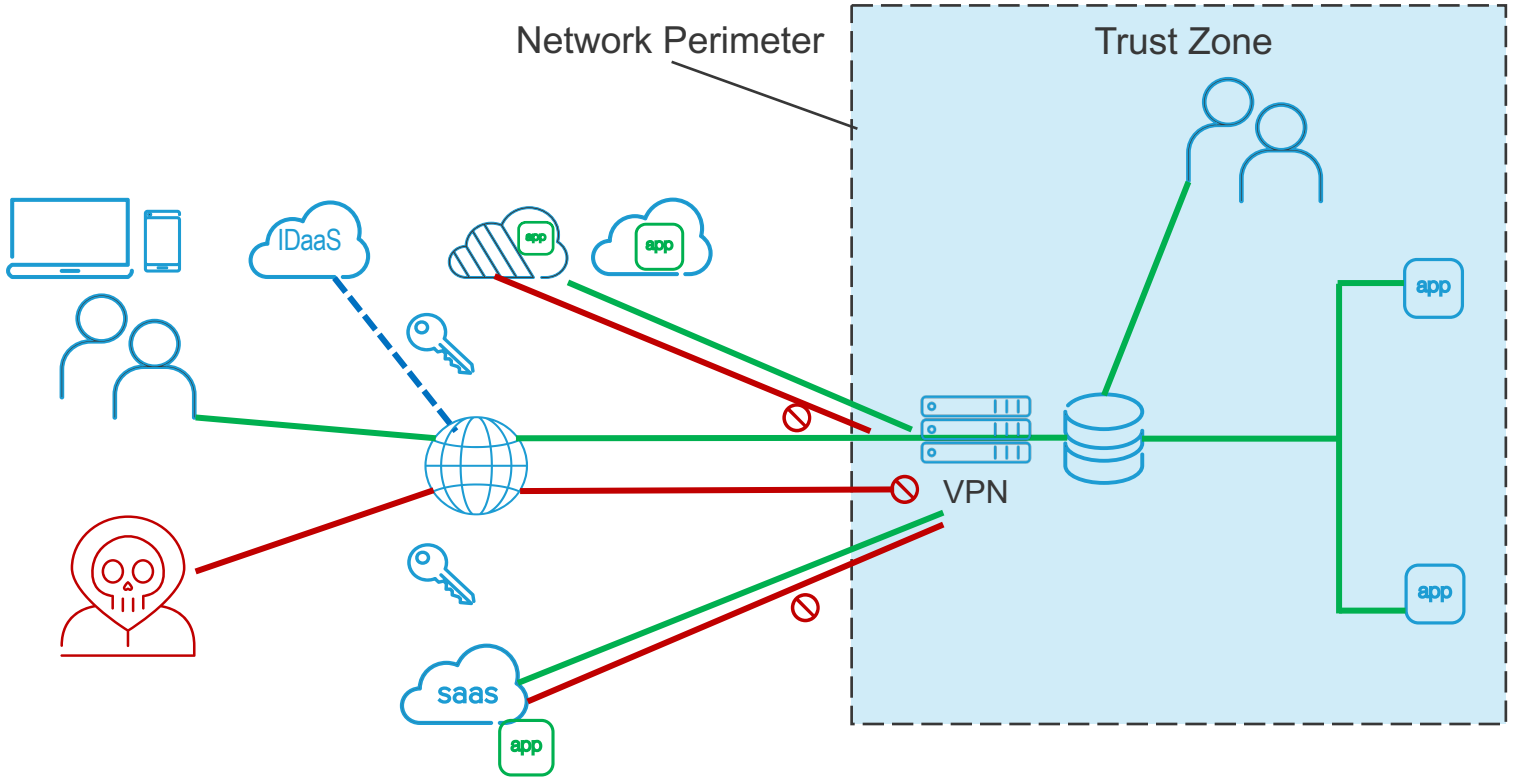
”Důvěřuj, ale prověřuj”

BEZPEČNOSTNÍ KONCEPT HRADU NA KOPCI



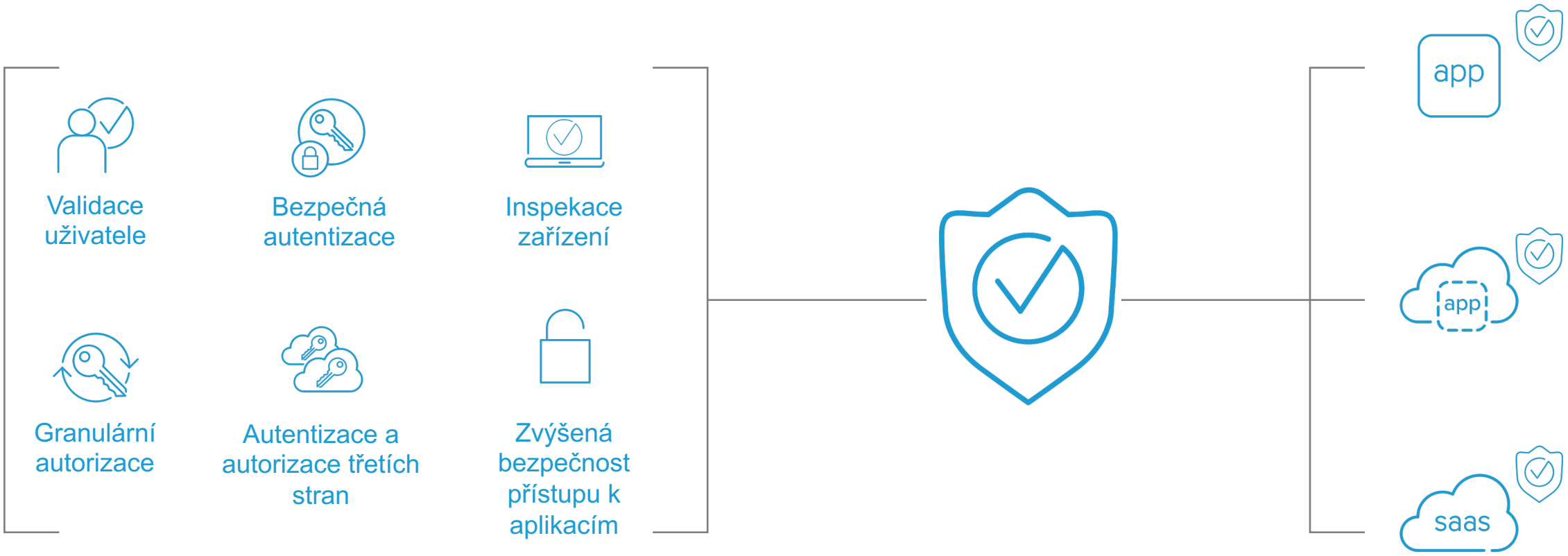
V dnešní době jsou služby často mimo perimeter

JAK PAK ŘEŠIT BEZPEČNOSTÍ KONCEPT PŘÍSTUPU K FIREMNÍM APLIKACÍM?



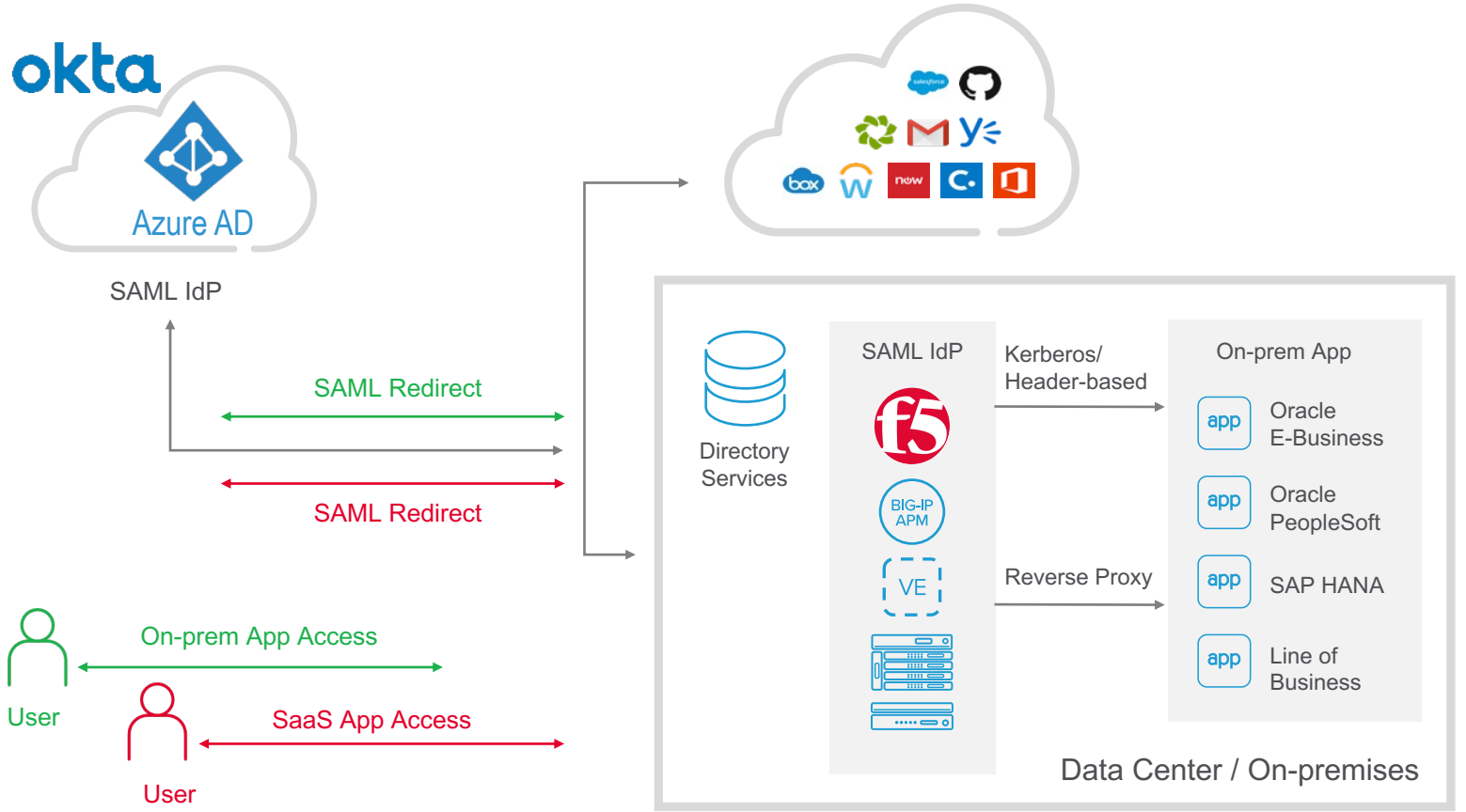
ZERO TRUST: Nikdy nedůvěřuj a vždy prověřuj!

“DŮVĚŘUJ, ALE PROVĚŘUJ” JE ZASTARALÝ BEZPEČNOSTNÍ CONCEPT
VPN SI NAVÍC DO CLOUDU NEVYTOČÍTE



Kompletní a uživatelsky přívětivý SSO k aplikacím

KRITICKÉ, ON-PREM A LEGACY APLIKACE



Rozšiřuje Microsoft Azure Active Directory single sign-on (SSO) a federaci

Modernizuje přístup k on-prem aplikacím

Zvyšuje bezpečnost

Microsoft

Reálné zkušenosti a doporučení z případů napadených českých nemocnic

Cílem je zvládnout situaci tak, aby se minimalizovaly ztráty
a redukoval čas obnovy a související náklady.

Příklad 1: Incident response v státní správě

1. IT zpozorovalo, že se něco děje přibližně **po 1 hodině**
2. Nastává fáze umírání infrastruktury, IT se bezprizorně dívá
3. První reakce na útok byla až po infikovaní více jak 50 % infrastruktury
4. Vypínají se virtuální stroje, trvá hodinu
5. Po vypnutí nikdo neví, co je infikováno a co ne
6. Vypínají se všechny síťové porty
7. Zálohy jsou smazány

Závěr:

Motiv neznámý, chybějí zálohy, máme data? Není možné vypátrat útočníka.

Nevíme co dál.

Příklad 2: Incident response ve finanční instituci

1. Zákazník zjišťuje anomálie na účtech
2. Po 1 měsíci jsou nalezeny stopy útočníka na interních serverech
3. Po 6 měsících útočník stále operuje ve společnosti, IT není schopno odstranit aktivity bez přerušení provozu a reputačních škod
4. Následně povolán externí IR team, nasazení nástroje a zastavení aktivit útočníka do 4h
5. Cílené pozorování aktivit útočníka, zjišťuje se motiv a forenzní stopy
6. Úplné zastavení útočníka a jeho eradikace

Závěr:

Nízká úroveň bezpečnosti a kompetence IT a managementu

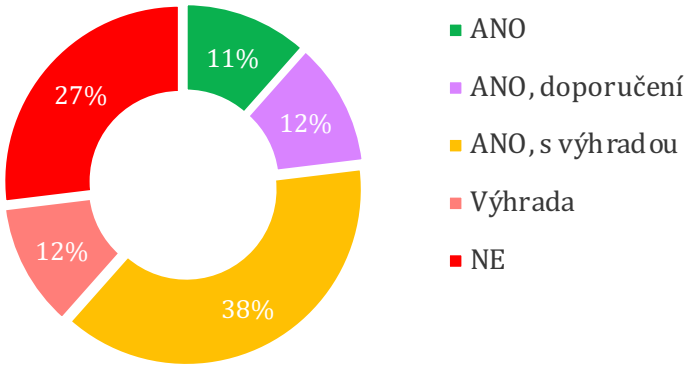
Pomalé reakce

Jak se na útok připravit?

- Ochrana internetového perimetru
- Pokročilá ochrana stanic a serverů
- Bezpečné zálohy a plán obnovy
- Management zranitelností a hardening
- Orchestrace a automatizace
- Expertní znalost

Požadavky VyKB

Celkové hodnocení rozdílové GAP analýzy po oblastech



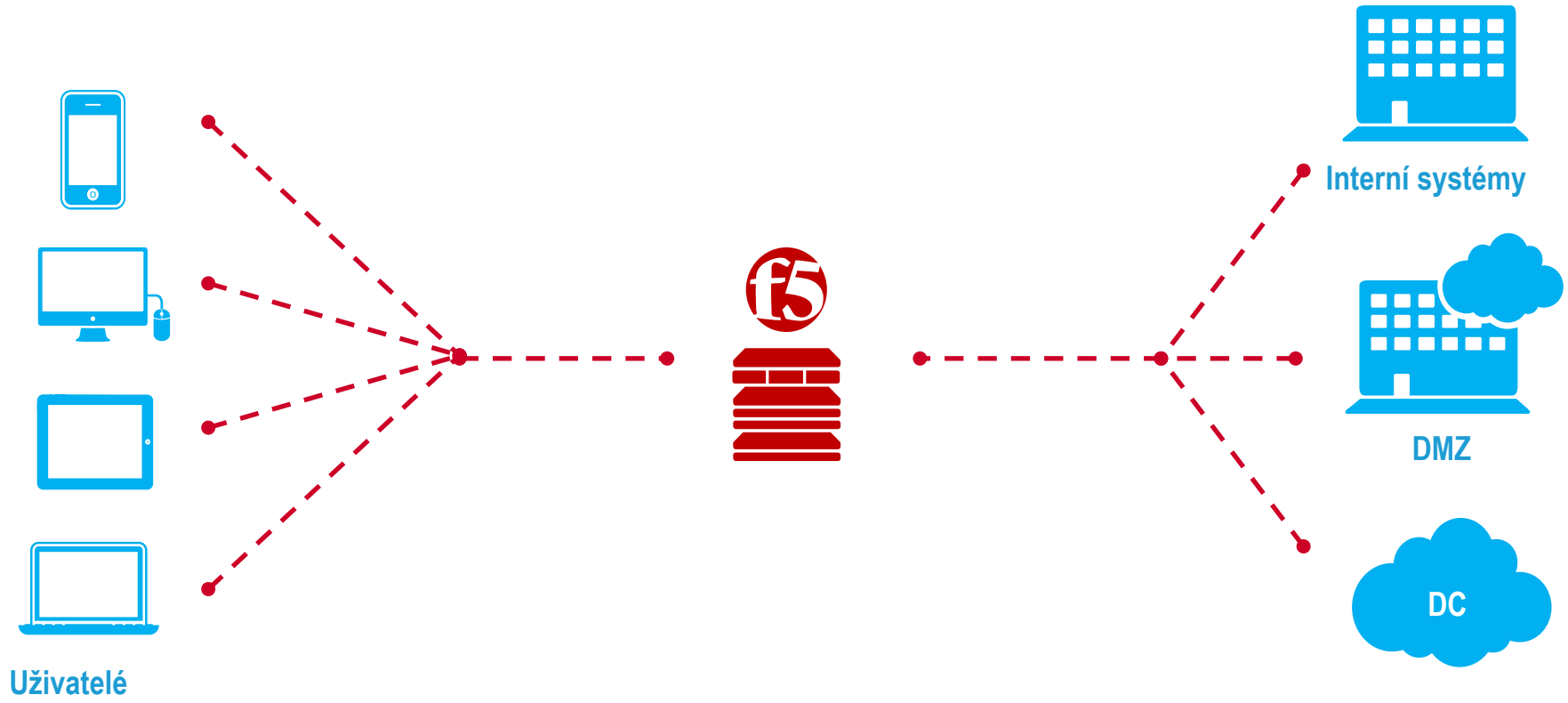
- § 19 Správa a ověřování identit - Nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací

- § 25 Aplikační bezpečnost - Povinná osoba dále v rámci aplikační bezpečnosti zajistí **trvalou** ochranu aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností.

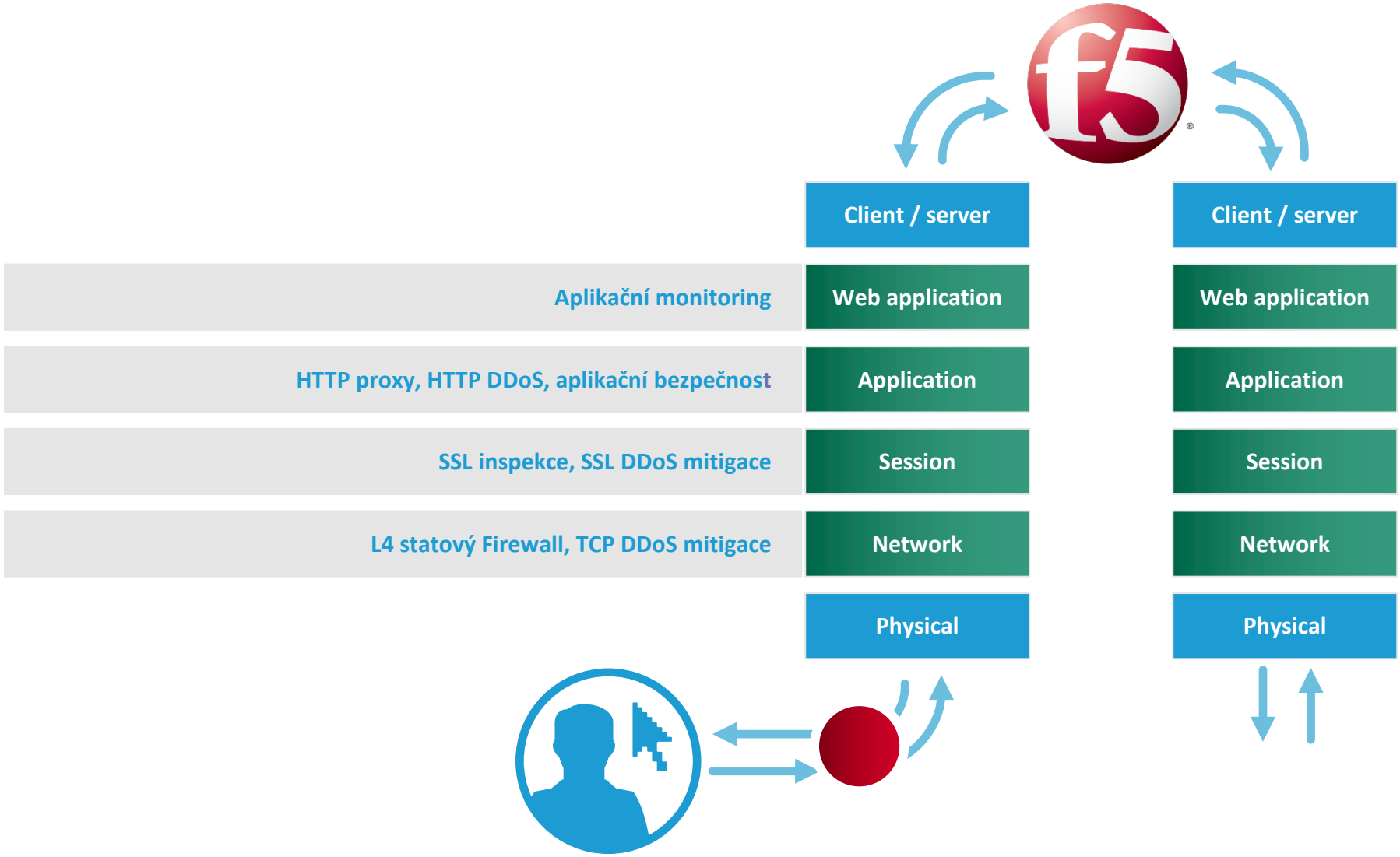
- § 26 Kryptografické prostředky - Povinná osoba pro ochranu aktiv informačního a komunikačního systému používá aktuálně odolné kryptografické algoritmy a kryptografické klíče, používá systém správy klíčů a certifikátů

- § 27 Zajišťování úrovně dostupnosti informací - odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost,

WAF a její místo



Kde probíhá inspekce?



Funkce loadbalanceru a WAF

Vysoká dostupnost

Bezpečné a rychlé webové služby

- HTTP 2.0, TLS 1.3 a hardening

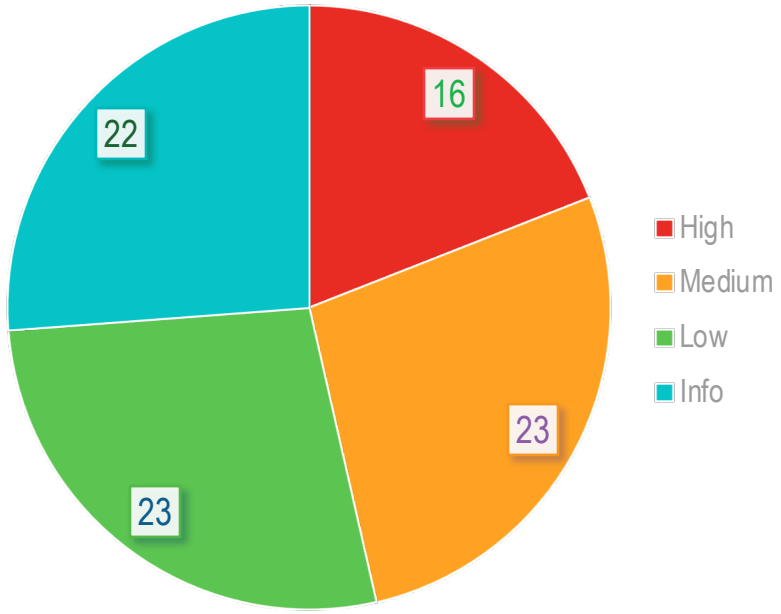
Single-sign-on, autentizační brána

Ochrana kritických aplikací v internetu a interní síti

Eliminace nálezů z PT v aplikacích

Nejčastější bezpečnostní problémy

- SQL Injekce
- Cross-Site Scripting (XSS)
- Slabý autentizační formulář
- Únik citlivých dat
- Path Traversal / Directory listing
- Zranitelnost REST API a SOAP
- Chyby v business logice
- Krádež SESSION
- Zranitelnosti aplikačních serverů, aplikací a externích knihoven
- Nedostatečná bezpečnostní znalost ve vývojovém týmu



SQL Injekce

Zranitelný kód:

```
<?php
function save_message($user, $message)
{
    $sql = "INSERT INTO Messages (
              user, message
            ) VALUES (
              '$user', '$message`
            )";
    return mysql_query($sql);
} ?>
```

Kód útočníka:

```
test');DROP TABLE Messages;--
```

Výsledek:

```
INSERT INTO Messages (user, message) VALUES (‘john’,’test’); DROP TABLE Messages;-- )”;
```

Cross-Site scripting

Zranitelný kód:

```
<?php
    $user = $_COOKIE['user'];
    $message = $_REQUEST['message'];
    if($message) {
        save_message($user, $message);
    }
?>
<input type="text" name="message" value="<?php echo $message ?>">
```

Kód útočníka:

```
<script type="text/javascript">
  var adr = '../evil.php?cakemonster=' + escape(document.cookie);
</script>
```

Výsledek:

```
<input type="text" name="message" value=""><script type="text/javascript"> var adr =
'../evil.php?cakemonster=' + escape(document.cookie);</script><input type=hidden value=””>
```

A co třeba vzdálený přístup?

Uživatelská VPN

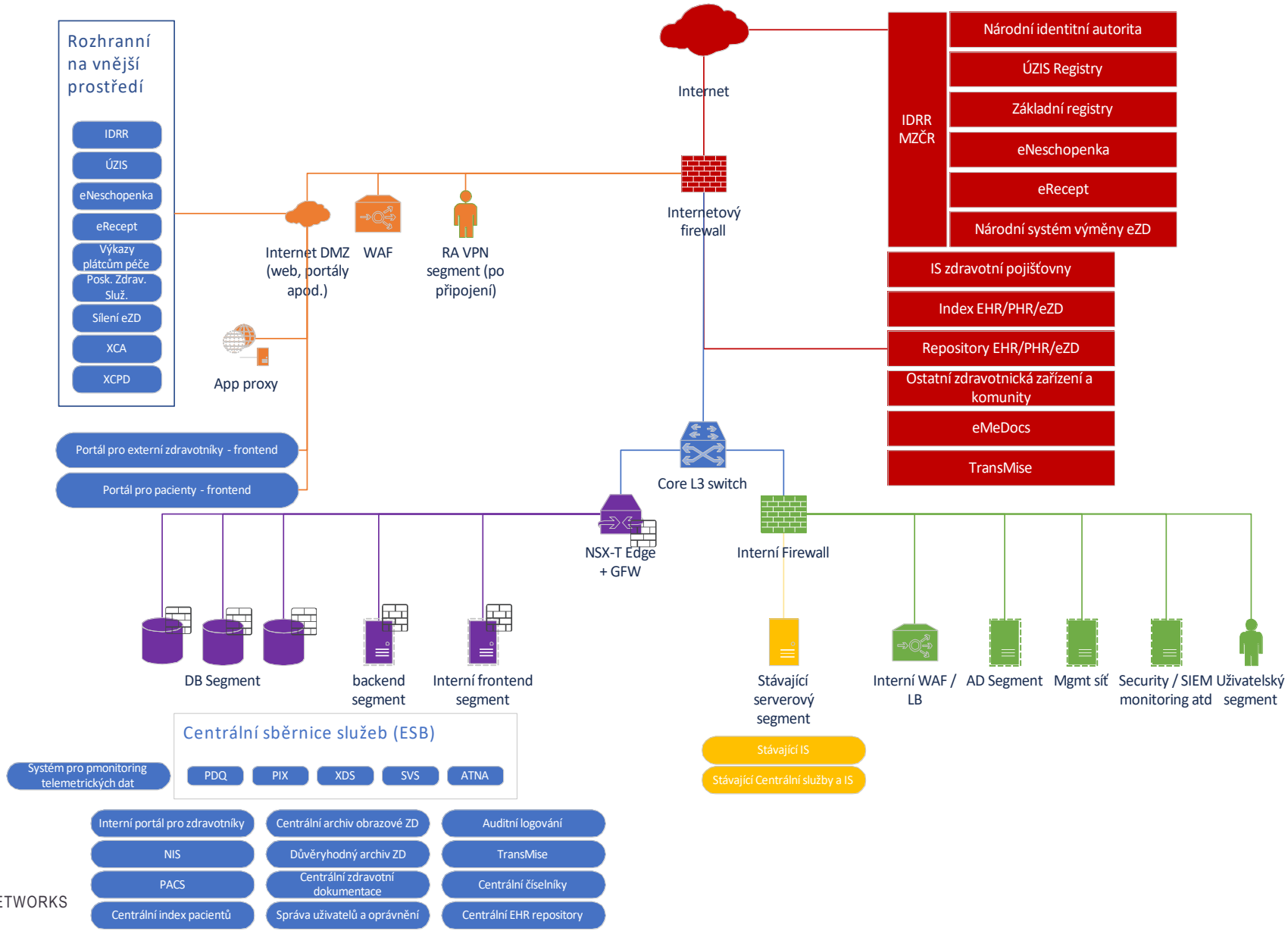
Bezpečná publikace interních aplikací

Autentizace na doménu, SAML, …

Nativní podpora autentizace a autorizace s o365, využití Conditional Access

Vynucení MFA

Vzorová architektura



Co se změní implemetací F5?

Shoda v rámci ZoKB
§19, §25, §26, §27

Okamžitá eliminace TOP bezpečnostních problémů

Vyšší viditelnost a schopnost předvídat útok

Nezávislost na vývojovém týmu a verzích SW třetích stran

SOLUTIONS & PRODUCTS PARTNERS RESOURCES SUPPORT COMPANY GET F5

Datum a čas: Úterý, 20. září 2022 | 8:30 - 16:30
Místo: Hotel Stages, Českomoravská 19a, 190 00 Praha 9

Září bude našlapané konferencemi, proto bychom Vás už nyní rádi pozvali na **F5 Solution Day**, který se bude konat v úterý **20. září** v nových prostorech **hotelu Stages**.

https://www.f5.com/c/emea-2022/event/f5-solution-day-prague

f.kolar@f5.com