elis consulting

Konzultace a poradenství

Naším posláním je pomáhat firmám a poskytovatelům služeb zorientovat se v džungli moderních technologií, AI a kybernetické bezpečnosti

NETWORKING ROADSHOW 2025

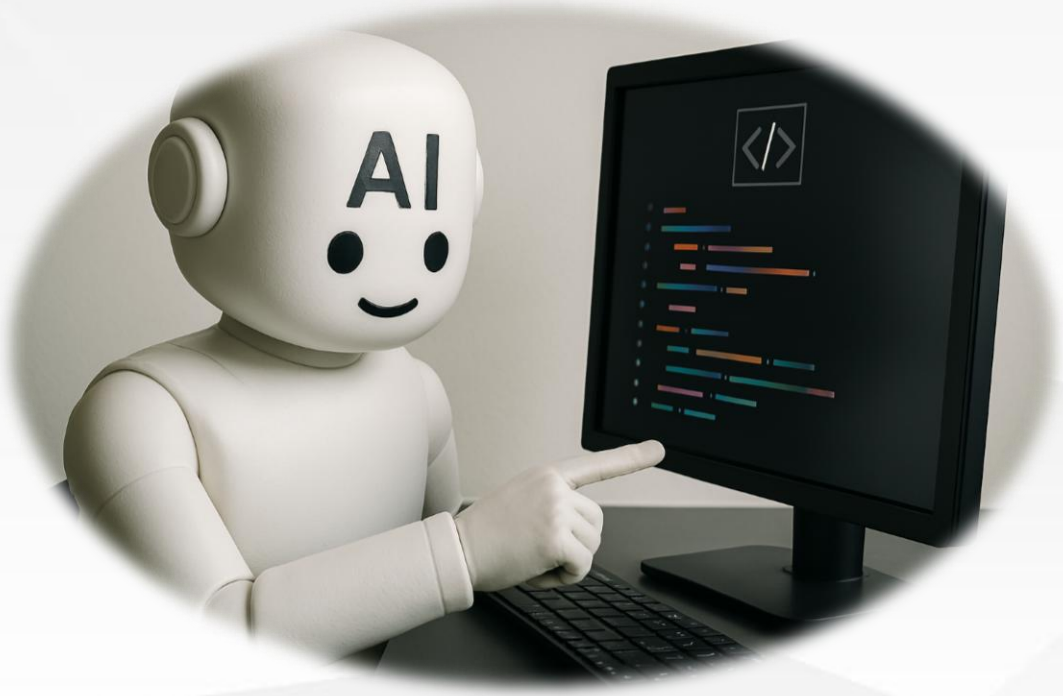
Výběr aktuálních kybernetických hrozeb a bezpečnostní rizika související s AI

Marek Mikuš
Lucie Skryjová

08.04.2025

1 Dva největší akcelerátory kybernetických útoků

Umělá Inteligence

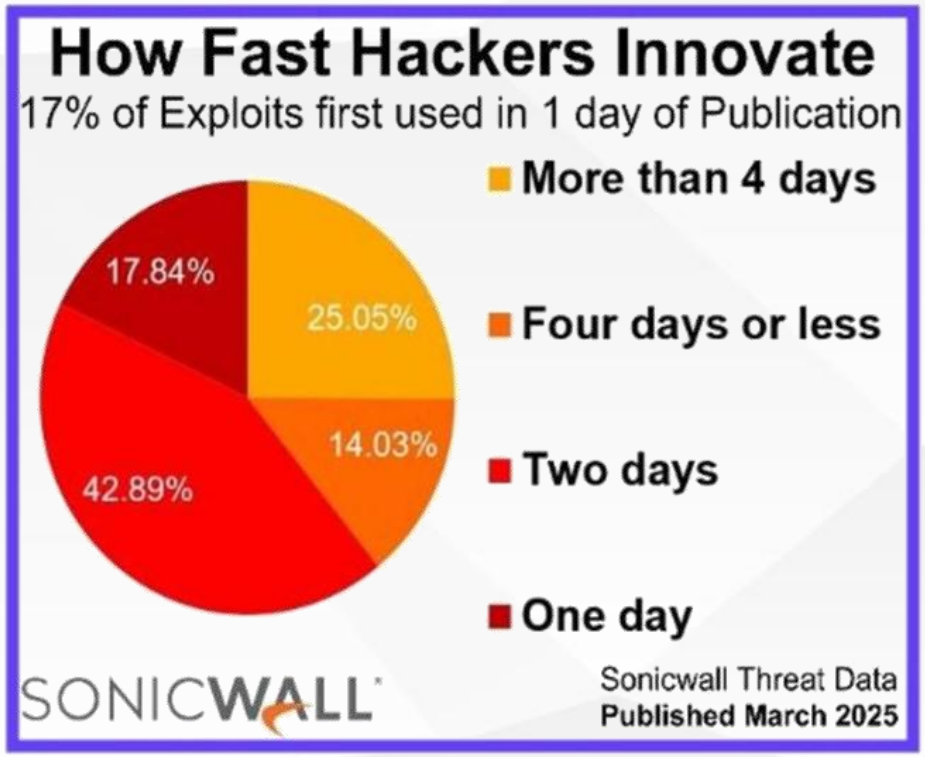


Zdroj : OpenAI

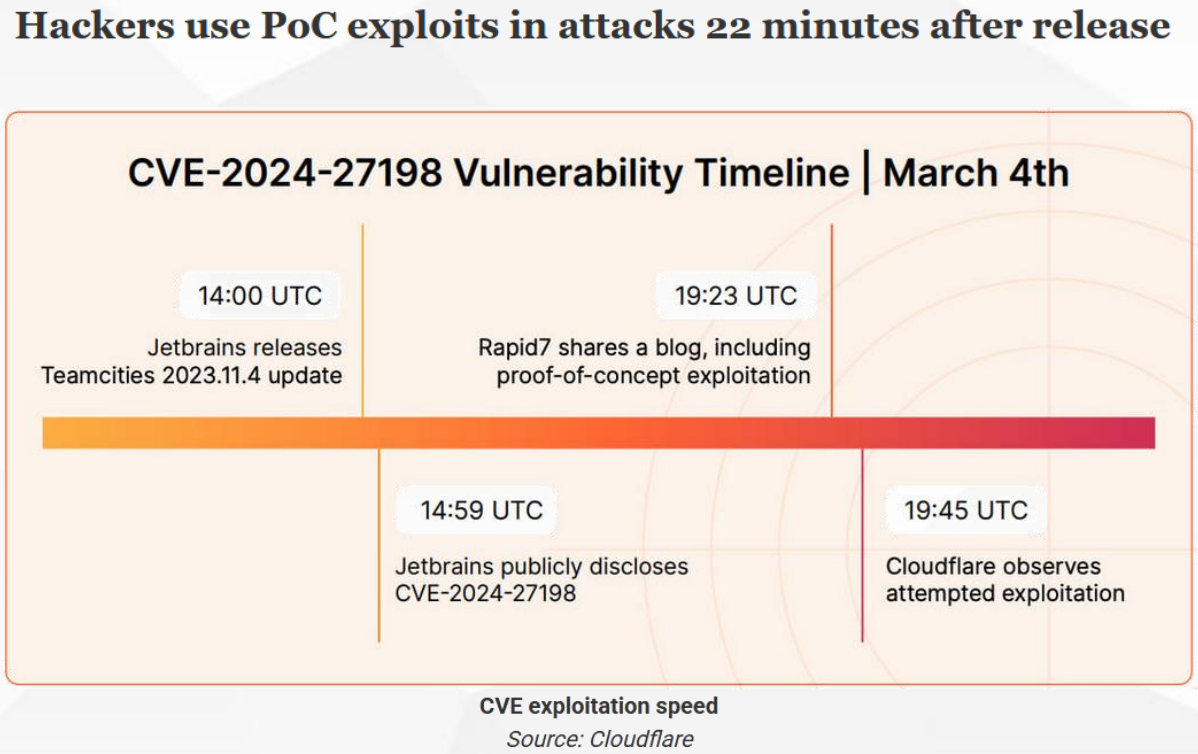
Geopolitická situace

elis consulting

1 Rychlost adopce hackerských skupin na nové zranitelnosti



Zdroj : Sonicwall



elis consulting

2 Reálné dopady na reputaci kvůli heslu

elis consulting

2 Reálné technické dopady kvůli heslu

RIPE Account Hacking Leads to Major Internet Outage at Orange Spain

Orange Spain's internet went down for several hours after its RIPE account was hacked, likely after malware stole the credentials.

By Eduard Kovacs
January 4, 2024

Orange Spain customers were unable to access the internet for several hours on January 3 as a result of a hacker attack that appears to have involved credentials stolen by malware.

ars TECHNICA SUBSCRIBE SIGN IN

COMEDY OF ERRORS —

A "ridiculously weak" password causes disaster for Spain's No. 2 mobile carrier

BGP tampering caused by poor security hygiene causes major outage for Orange España.

DAN GOODIN - 1/5/2024, 1:01 AM

Enlarge

Orange España, Spain's second-biggest mobile operator, suffered a major outage on Wednesday after an unknown party obtained a "ridiculously weak" password and used it to access an account for managing the global routing table that controls which networks deliver the company's Internet traffic, researchers said.

elis consulting

2 Reálné dopady na reputaci kvůli Supply chain

SOURCE: ANATOLY VARTANOV VIA ALAMY STOCK PHOTO

NEWS BRIEF

Volkswagen Group experienced a data breach last month, exposing sensitive personal information of roughly 800,000 electrical vehicle owners across its brands, including Volkswagen, Audi, Seat, and Skoda.

Initially reported by German publication Speigel, the breach has been attributed to an Amazon cloud storage system misconfiguration, which is managed by software subsidiary Cariad. The group reportedly left personal and location data openly accessible online for months on end, prompting the breach.

The anonymous hacker who discovered the breach reported it to Chaos Computer Club (CCC), a well known organization of ethical hackers in Europe. The CCC tested the open, insecure access before informing Cariad and Volkswagen.

The data exposed in the breach includes vehicle location information such as when EVs were switched on and off, along with location data, email addresses, phone numbers, and home addresses of car owners.

800,000 EV drivers' data exposed in Volkswagen breach

Article by **Gadjo Sevilla**
Jan 2, 2025

The news: **Cariad**, a **Volkswagen** subsidiary, leaked the personal data of 800,000 VW, **Audi**, **Seat**, and **Skoda** EV drivers. The leak included precise location data for 460,000 cars and personal information.

It's the latest setback to EV and connected car adoption, revealing how technology-dependent vehicles collect far too much personal data—which some security experts see as a privacy nightmare.

A bad start to VW's EV pivot: This incident compounds VW's challenges that already include sluggish EV sales and its recovery from the 2015 Dieselgate scandal.

- The leak, stored unencrypted on **Amazon Web Services** (AWS) cloud servers, was widely accessible for months and **affected EV owners including German politicians, business leaders, and the Hamburg police**, per Der Spiegel.
- The data included driver names, contact details, emails, phone numbers, addresses, and even **records of when and where EVs were switched on and off**.
- There is no evidence the leak was exploited, and Cariad assured EV owners that no action is needed to protect their data.
- The breach may challenge consumer trust in Volkswagen's digital offerings.

elis consulting

2 Reálné problémy kvůli Supply chain – FVE

VULNERABILITIES

We cataloged 93 previous vulnerabilities on solar power and analyzed trends:

There's an average of over **10 new vulnerabilities** disclosed per year in the past **3 years**

(15%) Relatively few vulnerabilities (15%) affect solar inverters directly

32% have a CVSS score of 9.8 or 10 which generally means an attacker can take full control of an affected system

80% of those have a high or critical severity

The most affected components are:

FOREIGN-MADE

Due to growing concerns over the dominance of foreign-made solar power components, we analyzed their common countries of origin:

53% of solar inverter manufacturers are based in China

The second and third most common countries of origin for components are:

2 India
3 US

58% of storage system

20% of the monitoring system manufacturers **are based in the same country**

NEW VULNERABILITIES

We analyzed **six of the top 10 vendors** of solar power systems worldwide:

1 Huawei 2 Sungrow 3 Ginlong Solis
4 Growatt 5 GoodWe 6 SMA

Some vulnerabilities also allow attackers to hijack other smart devices in users' homes

We found **46 new vulnerabilities** affecting different components in three vendors: Sungrow, Growatt and SMA.

1 Sungrow 2 Growatt 3 SMA

These vulnerabilities enable scenarios that impact grid stability and user privacy

Zdroj : Forescout Technologies

Vendor	Market share	Selected for analysis?
Huawei	29%	Yes
Sungrow	23%	Yes
Ginlong Solis	8%	Yes
Growatt	6%	Yes
GoodWe	5%	Yes
SMA	3%	Yes

#	Vendor	Summary results
1	Huawei	No issues found in limited analysis
2	Sungrow	Possible takeover of devices and data leak
3	Ginlong Solis	No issues found in limited analysis
4	Growatt	Possible takeover of accounts and devices and data leak
5	GoodWe	No issues found in limited analysis
6	SMA	Remote Code Execution on the cloud platform

elis consulting

3 Kdo je skutečný cíl?

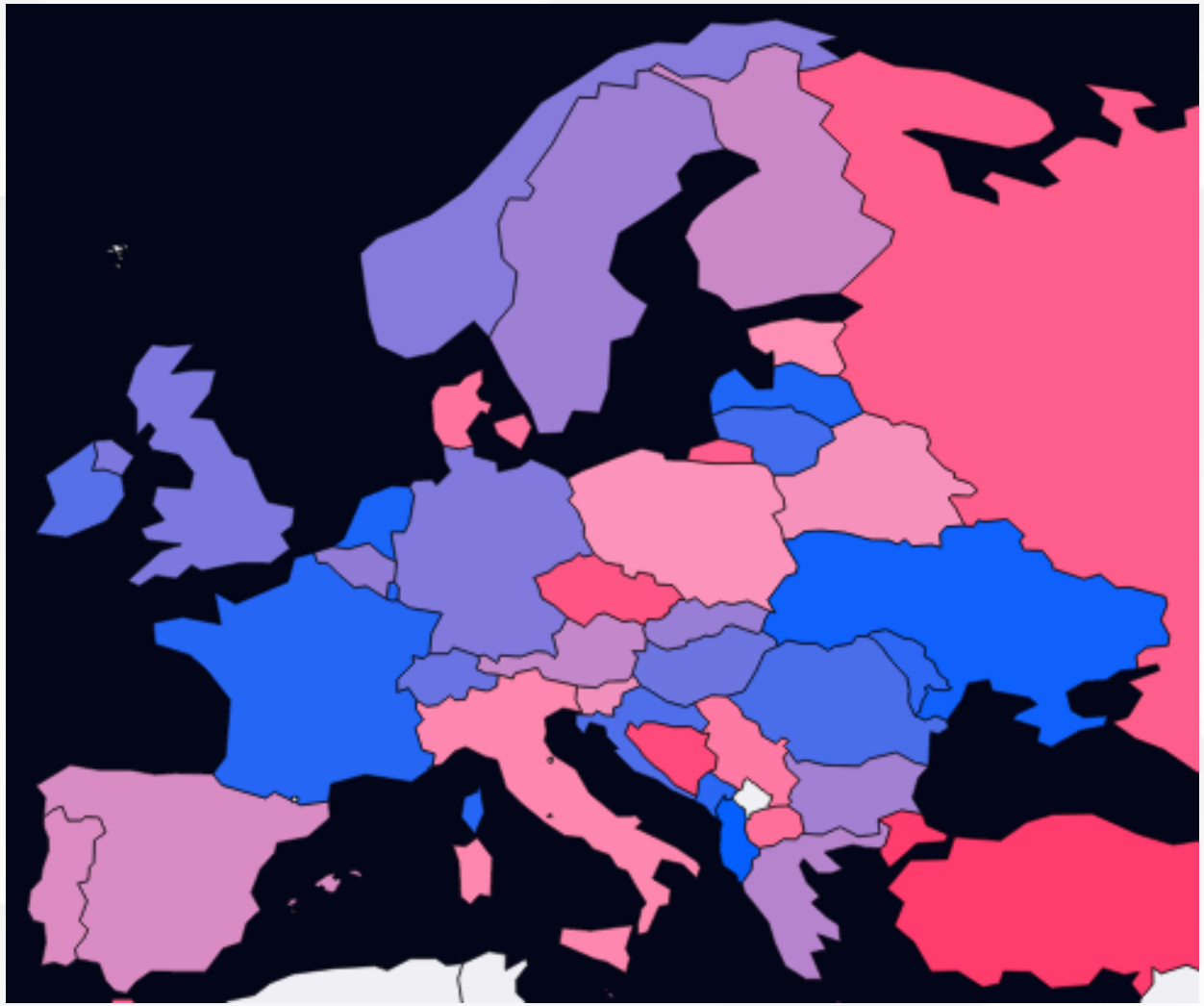
Vaše společnost

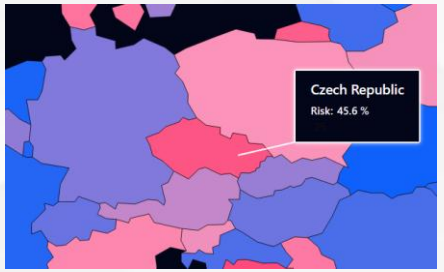
Váš dodavatel

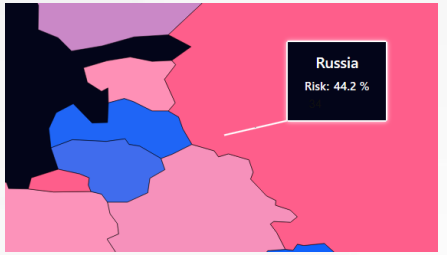
Váš zákazník

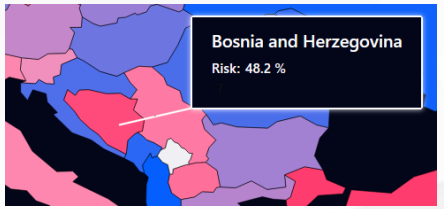
elis consulting

4 Globální analýza kybernetických rizik





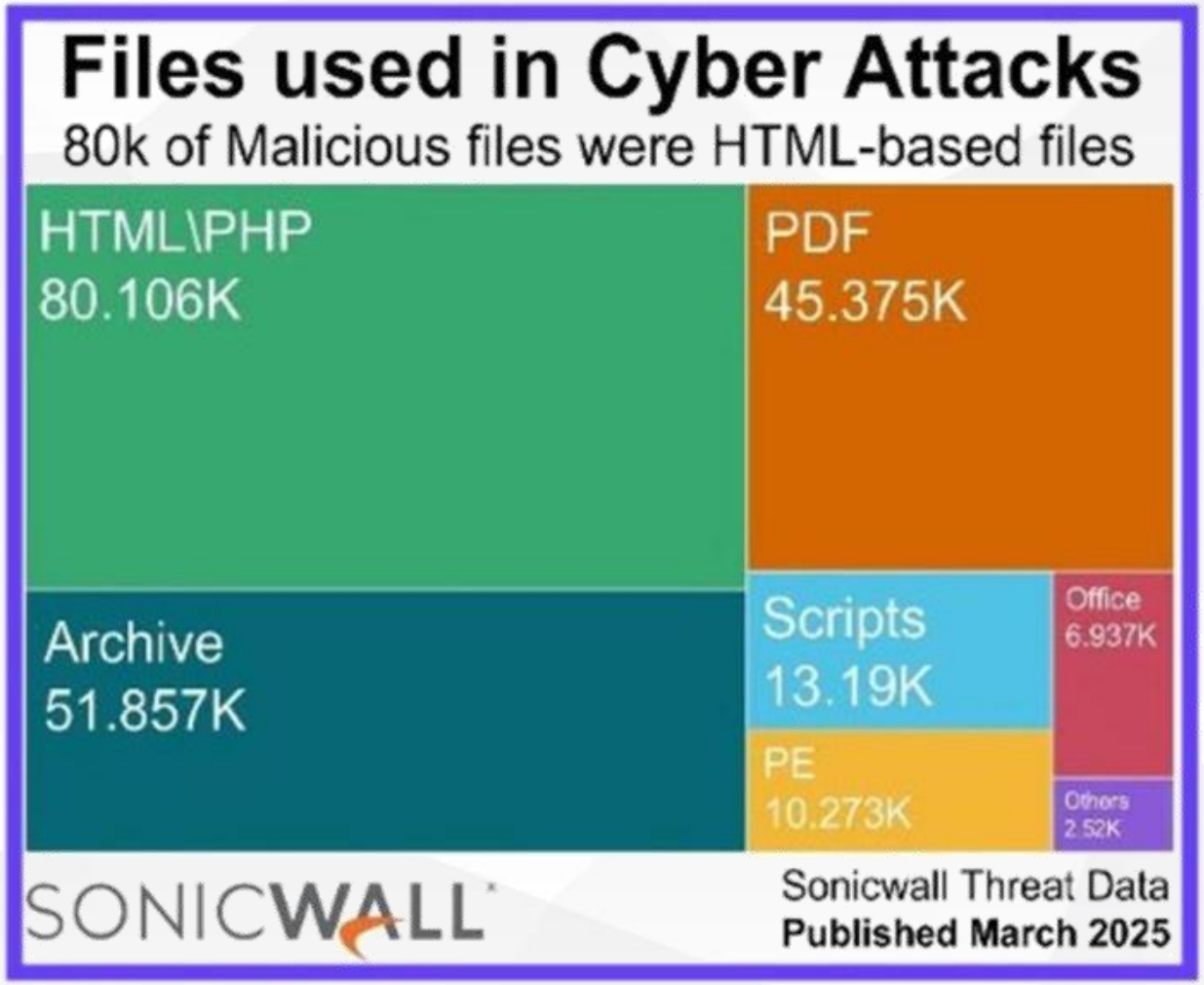




Zdroj : Check Point Software Technologies, Cyber Security Report 2023

elis consulting

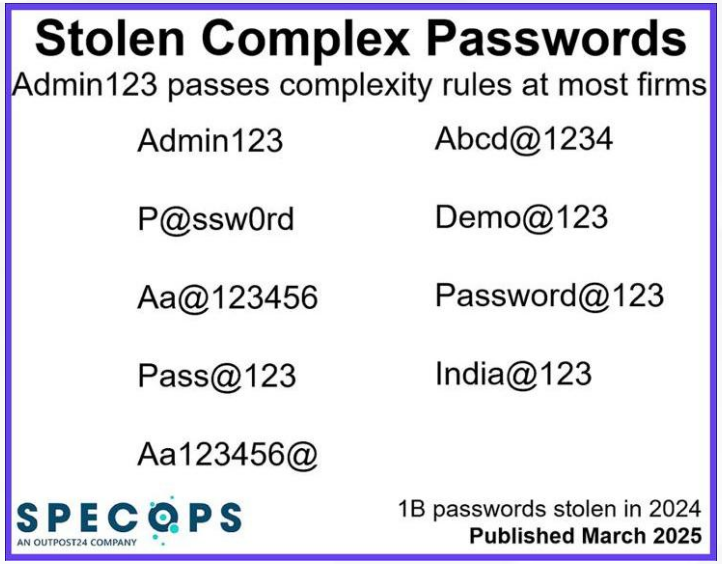
4 Nejčastěji zneužívané typy souborů

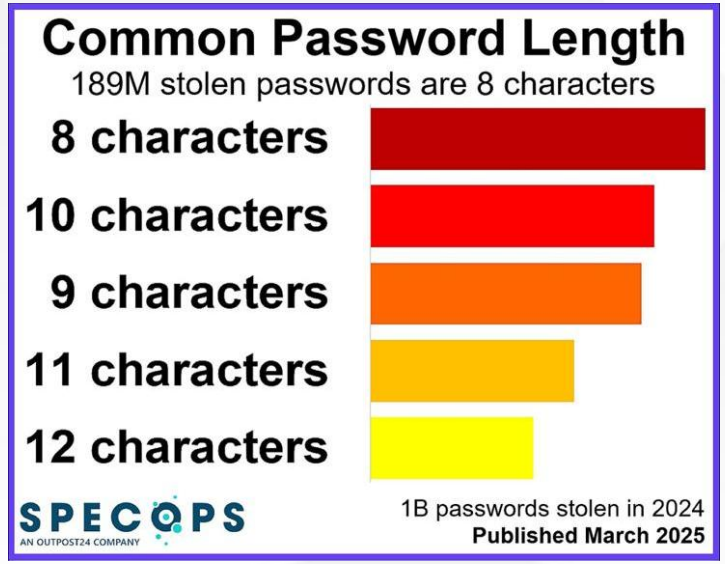


Zdroj : Sonicwall

elis consulting

5 Hesla a jejich dnešní běžný stav





Zdroj: Specops Weak Password Report, březen 2025

elis consulting

6 Nejtypičtější kyberhrozby

01 Phishing

02 Spear-phishing

03 Smishing

04 Vishing

05 Quishing

06 Zneužití Captcha

07 Tailgating

08 AI Deepfake

09 Baiting

10 Page hijacking

11 Ransomware Infostealery

12 IoT

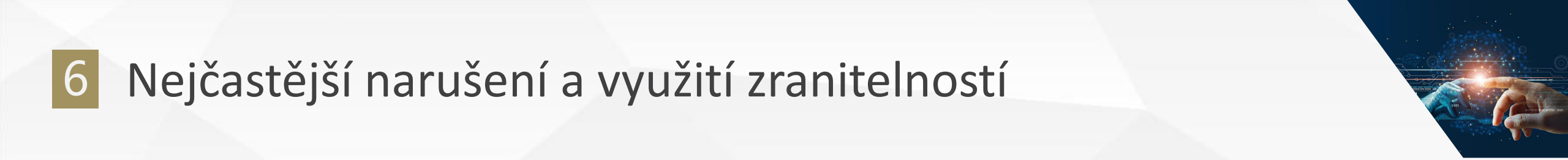
13 BEC

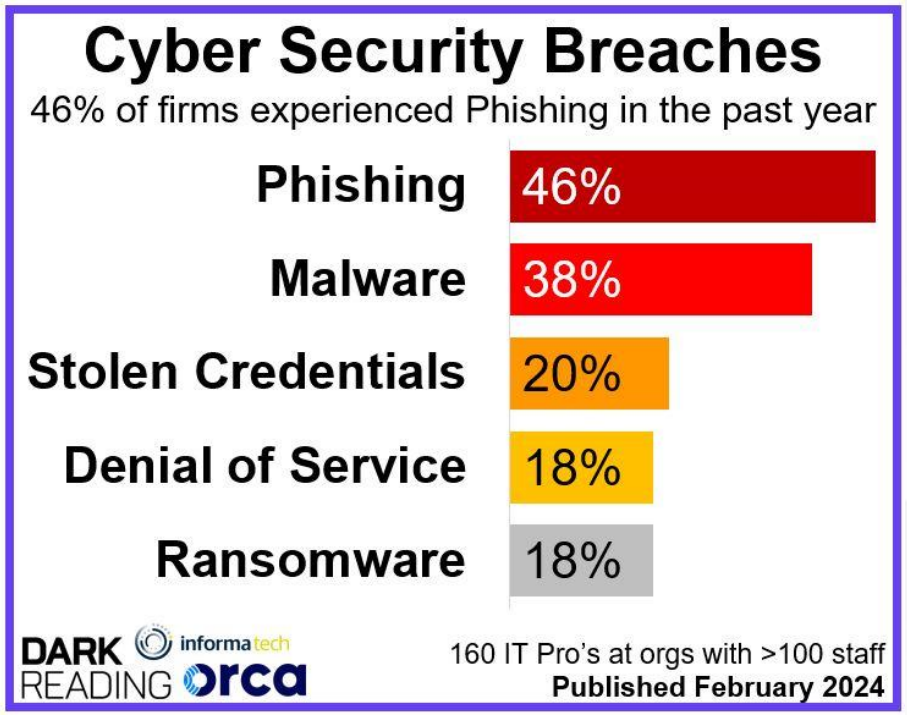
14 PWA

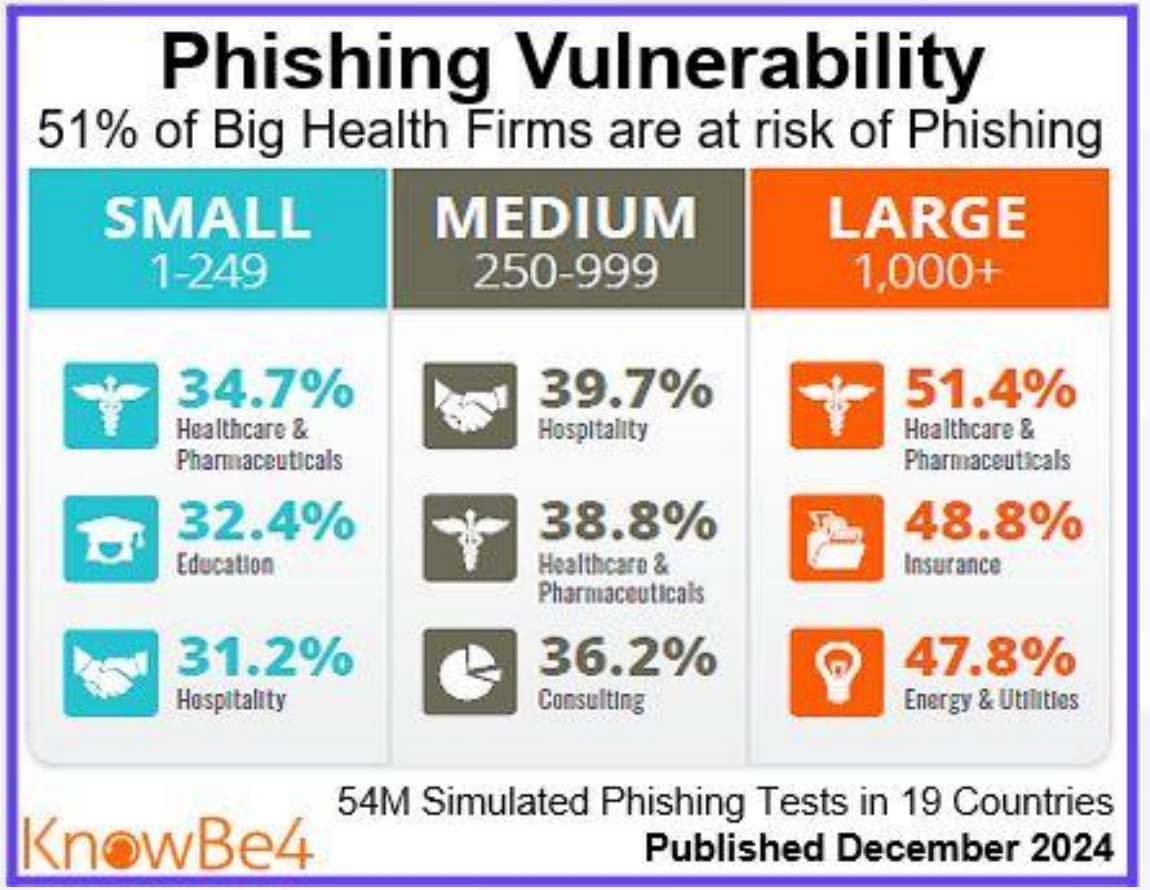
15 Wi-fi a Captive portal

elis consulting

6 Nejčastější narušení a využití zranitelností



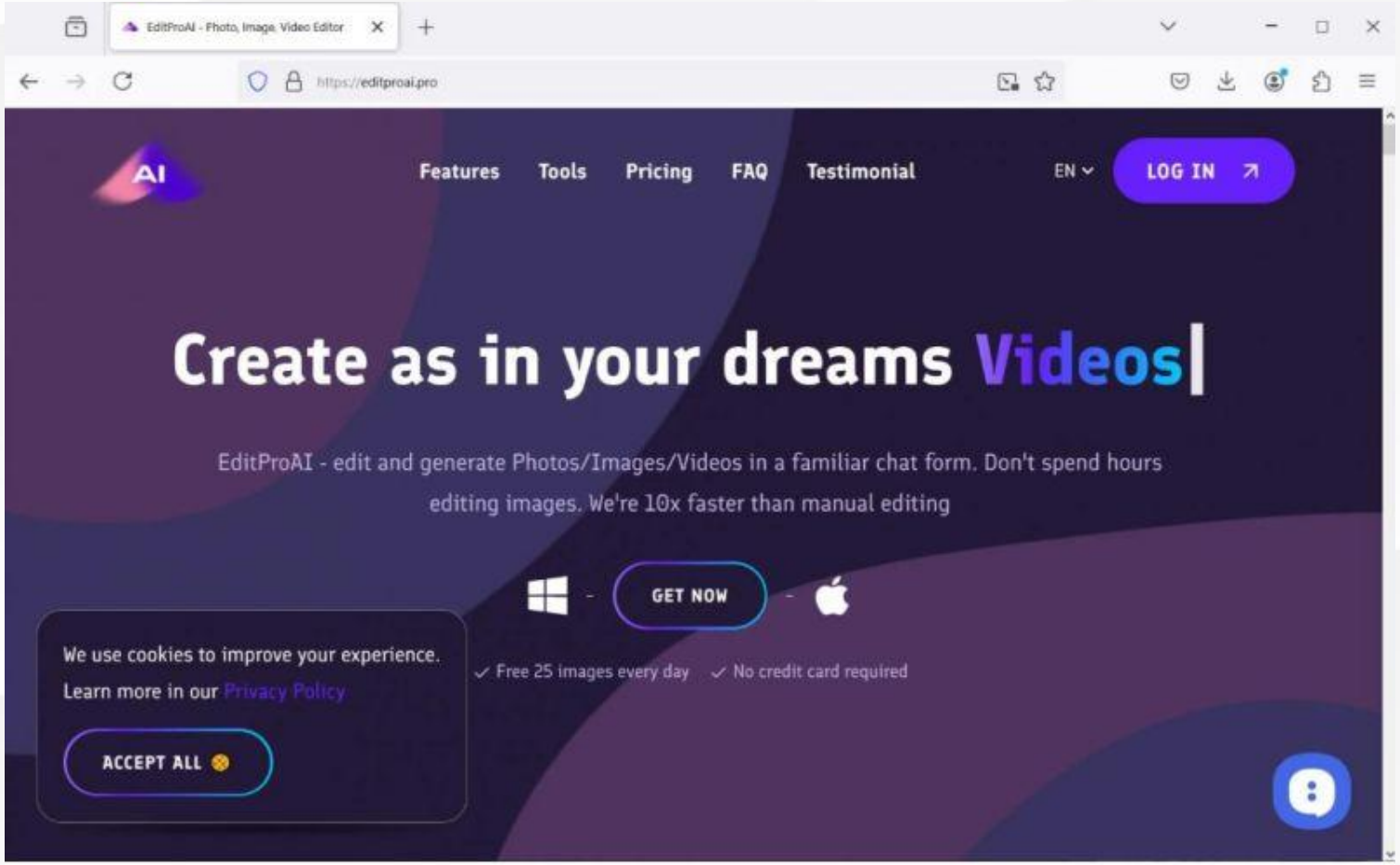




elis consulting

6 Page hijacking u AI

Varování před EditProAI



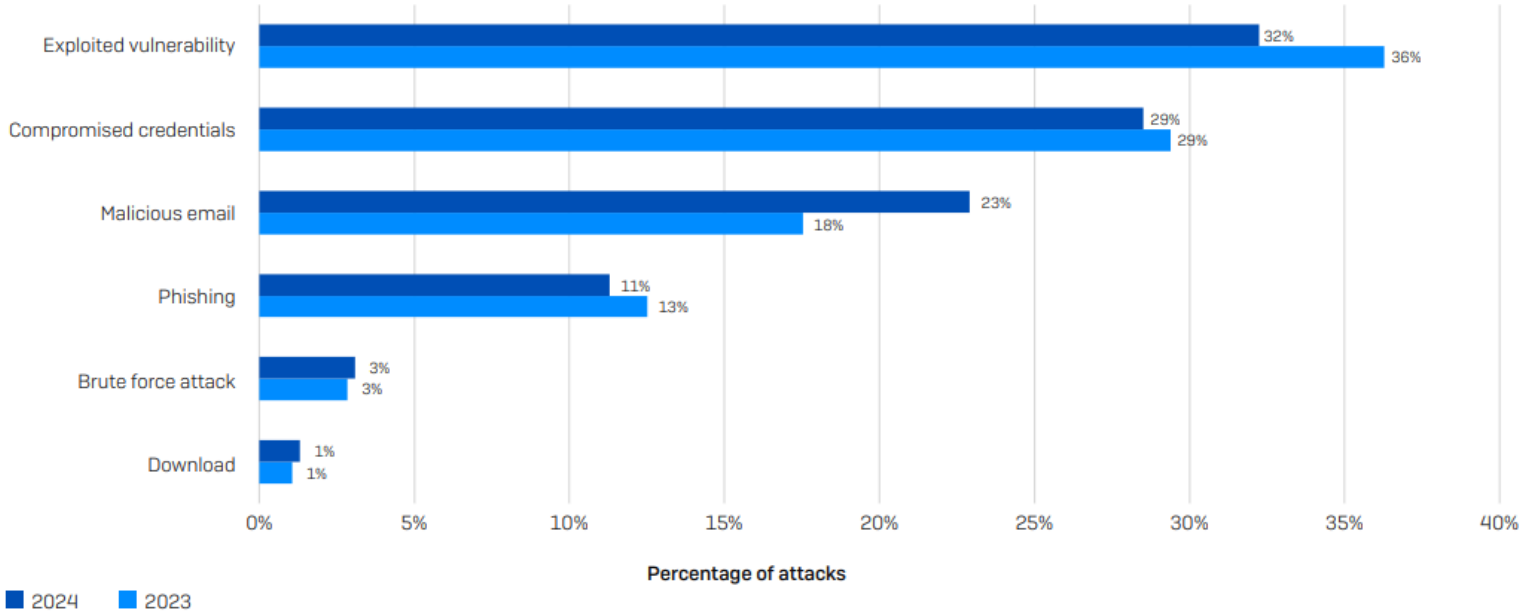
elis consulting

6 Ransomware – Data od Sophos z roku 2024

Root Causes of Ransomware Attacks

99% of organizations hit by ransomware were able to identify the root cause of the attack, with exploited vulnerabilities the most commonly identified starting point for the second year running. Overall, the running order remained consistent with our 2023 study.

Email-based approaches were identified as the root cause of attack by 34% of respondents, with around twice as many starting with a malicious email (i.e., a message with a malicious link or attachment that downloads malware) as phishing (i.e., a message designed to trick readers into revealing information). It's worth noting that phishing is typically used to steal log-in details and as such can be considered the first step in a compromised credentials attack.



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=2,974 organizations hit by ransomware.

elis consulting

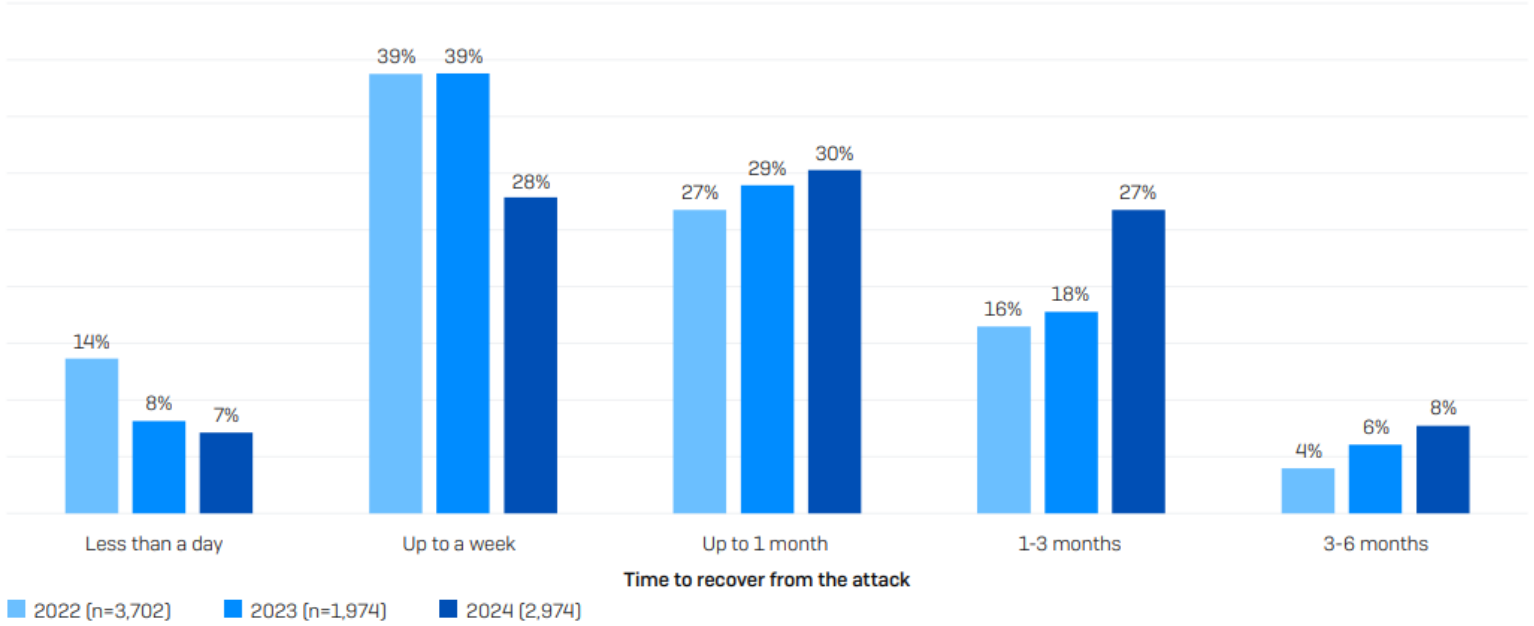
6 Ransomware – Data od Sophos z roku 2024

Recovery Time

The time taken to recover from a ransomware attack is getting steadily longer. Our 2024 research revealed:

- 35% of ransomware victims are fully recovered in a week or less, down from 47% in 2023 and 52% in 2022
- One third (34%) now take more than a month to recover, up from 24% in 2023 and 20% in 2022

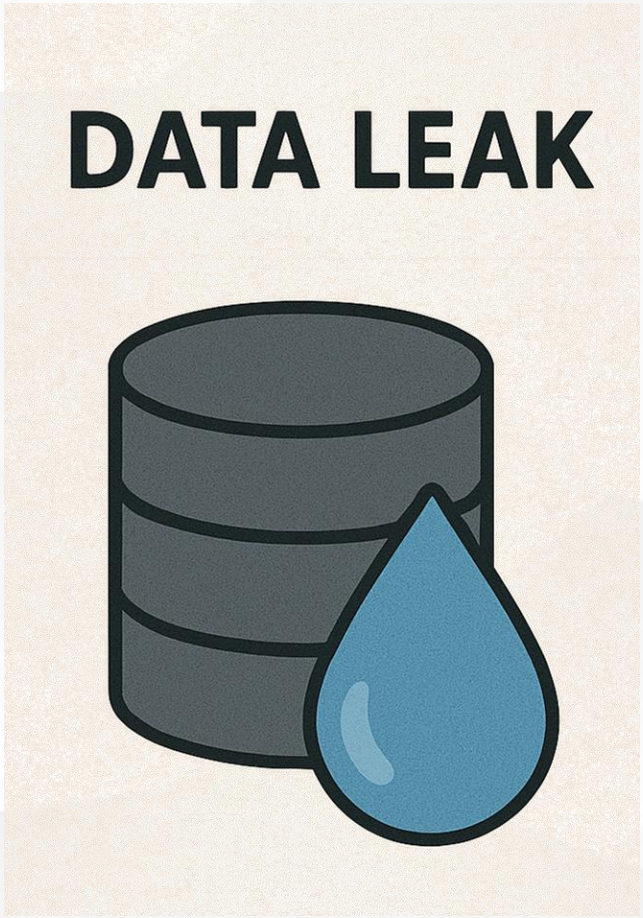
This slowdown may reflect the increased complexity and severity of attacks, necessitating greater recovery work. It may also indicate a growing lack of recovery preparation.



How long did it take your organization to fully recover from the ransomware attack? Base number in chart.

elis consulting

7 Infostealery cílí na VPN, Crypto, Hesla, Klienty, Cookies

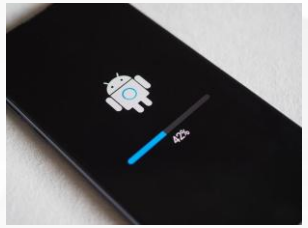


Zdroj : Open AI

elis consulting

7 Bezpečnostní doporučení – Aktualizace

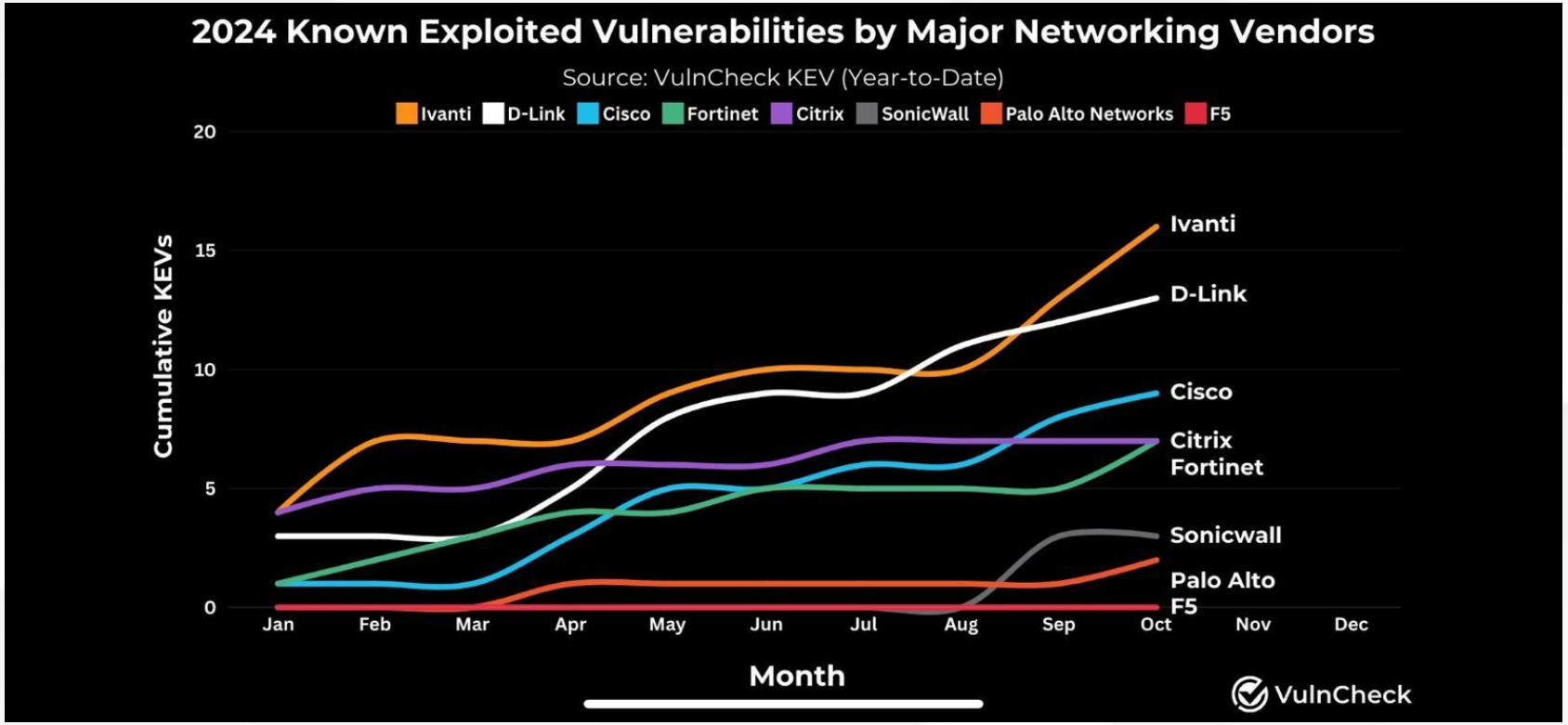
Neodkládejte aktualizace jakýchkoliv vámi používaných operačních systémů a aplikací (SW), stejně tak fyzických zařízení HW, pokud výrobce vydá bezpečnostní opravu.



elis consulting

7 Bezpečnostní doporučení

Neodkládejte aktualizace jakýchkoliv vámi používaných operačních systémů a aplikací (SW), stejně tak fyzických zařízení HW, pokud výrobce vydá bezpečnostní opravu.

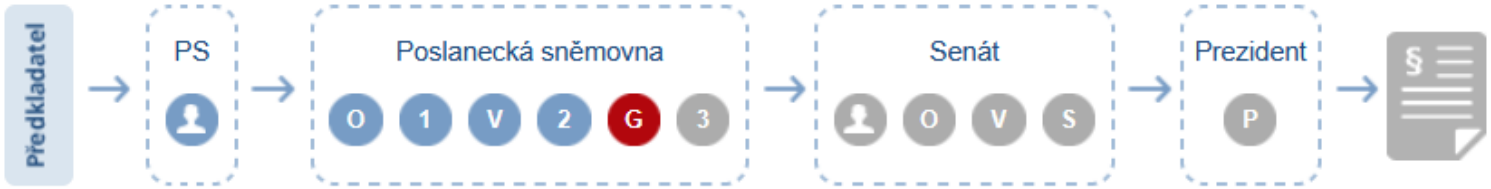


8 Stav nZKB v ČR

Sněmovní tisk 759
Vládní návrh zákona o kybernetické bezpečnosti - EU

Stav projednávání ke dni: 7. dubna 2025

Vysvětlení legislativního procesu



PŘEDKLADATEL

Vláda **předložila** sněmovně návrh zákona 25. 7. 2024.
Zástupce navrhovatele: předseda vlády.

Zdroj : Poslanecká sněmovna ČR

elis consulting

8 Stav nZKB v ČR

POSLANECKÁ SNĚMOVNA

Návrh zákona rozeslán poslancům jako tisk **759/0** dne 25. 7. 2024.
Návrh zaevidován v systému **eKLEP** pod čj. OVA **68/24**, PID ALBSCSSFKU7S.

Předsedkyně sněmovny projednání zákona **doporučila** 13. 8. 2024. Určila zpravodaje: Petr Letocha a navrhla přikázat k projednání výborům: Výbor pro bezpečnost (rozhodnutí č. 75)

O **Organizační výbor** projednání návrhu zákona **doporučil** 29. 8. 2024 (usnesení č. 296).
Navrhl Výbor pro bezpečnost jako garanční a navrhl přikázat k projednání dalšímu výboru: Hospodářský výbor.

1 Čtení proběhlo 17. 9. 2024 na 112. schůzi.
Návrh zákona **přikázán k projednání** výborům (usnesení č. 1114).

V
- Výbor pro obranu projednal návrh zákona a vydal 25. 9. 2024 **usnesení** doručené poslancům jako tisk 759/1 *(přerušuje projednávání)*.
- Garanční Výbor pro bezpečnost projednal návrh zákona a vydal 27. 9. 2024 **usnesení** doručené poslancům jako tisk 759/2 *(přerušuje projednávání)*.
- Hospodářský výbor projednal návrh zákona a vydal 27. 9. 2024 **usnesení** doručené poslancům jako tisk 759/3 *(přerušuje projednávání)*.
- Výbor pro obranu projednal návrh zákona a vydal 6. 11. 2024 **usnesení** doručené poslancům jako tisk 759/4 *(doporučuje schválit)*.
- Hospodářský výbor projednal návrh zákona a vydal 8. 11. 2024 **usnesení** doručené poslancům jako tisk 759/5 *(přerušuje projednávání)*.
- Garanční Výbor pro bezpečnost projednal návrh zákona a vydal 8. 11. 2024 **usnesení** doručené poslancům jako tisk 759/6 *(přerušuje projednávání)*.
- Hospodářský výbor projednal návrh zákona a vydal 29. 11. 2024 **usnesení** doručené poslancům jako tisk 759/7 *(pozměňovací návrhy)*.
- Garanční Výbor pro bezpečnost projednal návrh zákona a vydal 29. 11. 2024 **usnesení** doručené poslancům jako tisk 759/8 *(pozměňovací návrhy)*.

2 **2. Čtení** Návrh zákona **prošel** obecnou rozpravou 21. 1. 2025 na 127. schůzi.
Návrh zákona **prošel** podrobnou rozpravou 21. 1. 2025 na 127. schůzi.
Podané **pozměňovací návrhy** zpracovány jako tisk 759/9, který byl rozeslán 22. 1. 2025 v 10:54.

G
- Výbor pro bezpečnost vydal usnesení garančního výboru, které bylo 4. 4. 2025 doručeno poslancům jako sněmovní tisk 759/10 *(stanovisko)*.

Zdroj : Poslanecká sněmovna ČR

elis consulting

8 Stav nZKB v ČR

Sněmovní tisk 759
Vládní návrh zákona o kybernetické bezpečnosti - EU

Stav projednávání ke dni: 7. dubna 2025

Vysvětlení legislativního procesu

PŘEDKLADATEL

Vláda **předložila** sněmovně návrh zákona 25. 7. 2024.
Zástupce navrhovatele: předseda vlády.

POSLANECKÁ SNĚMOVNA

Návrh zákona rozeslán poslancům jako tisk **759/0** dne 25. 7. 2024.
Návrh zaevidován v systému **eKLEP** pod čj. OVA **68/24**, PID ALBSCSSFKU7S.

Předsedkyně sněmovny projednání zákona **doporučila** 13. 8. 2024. Určila zpravodaje: Petr Letocha a navrhla přikázat k projednání výborům: Výbor pro bezpečnost (rozhodnutí č. 75)

O **Organizační výbor** projednání návrhu zákona **doporučil** 29. 8. 2024 (usnesení č. 296).
Navrhl Výbor pro bezpečnost jako garanční a navrhl přikázat k projednání dalšímu výboru: Hospodářský výbor.

1 Čtení proběhlo 17. 9. 2024 na 112. schůzi.
Návrh zákona **přikázán k projednání** výborům (usnesení č. 1114).

V
- Výbor pro obranu projednal návrh zákona a vydal 25. 9. 2024 **usnesení** doručené poslancům jako tisk 759/1 *(přerušuje projednávání)*.
- Garanční Výbor pro bezpečnost projednal návrh zákona a vydal 27. 9. 2024 **usnesení** doručené poslancům jako tisk 759/2 *(přerušuje projednávání)*.
- Hospodářský výbor projednal návrh zákona a vydal 27. 9. 2024 **usnesení** doručené poslancům jako tisk 759/3 *(přerušuje projednávání)*.
- Výbor pro obranu projednal návrh zákona a vydal 6. 11. 2024 **usnesení** doručené poslancům jako tisk 759/4 *(doporučuje schválit)*.
- Hospodářský výbor projednal návrh zákona a vydal 8. 11. 2024 **usnesení** doručené poslancům jako tisk 759/5 *(přerušuje projednávání)*.
- Garanční Výbor pro bezpečnost projednal návrh zákona a vydal 8. 11. 2024 **usnesení** doručené poslancům jako tisk 759/6 *(přerušuje projednávání)*.
- Hospodářský výbor projednal návrh zákona a vydal 29. 11. 2024 **usnesení** doručené poslancům jako tisk 759/7 *(pozměňovací návrhy)*.
- Garanční Výbor pro bezpečnost projednal návrh zákona a vydal 29. 11. 2024 **usnesení** doručené poslancům jako tisk 759/8 *(pozměňovací návrhy)*.

2 **2. Čtení** Návrh zákona **prošel** obecnou rozpravou 21. 1. 2025 na 127. schůzi.
Návrh zákona **prošel** podrobnou rozpravou 21. 1. 2025 na 127. schůzi.
Podané **pozměňovací návrhy** zpracovány jako tisk 759/9, který byl rozeslán 22. 1. 2025 v 10:54.

G
- Výbor pro bezpečnost vydal usnesení garančního výboru, které bylo 4. 4. 2025 doručeno poslancům jako sněmovní tisk 759/10 *(stanovisko)*.

Zdroj : Poslanecká sněmovna ČR

Projednávání tisku navrženo na pořad 136. schůze (od 15. dubna 2025), ale přihlášeno zatím není...

136. schůze

Zákony

1. Vládní návrh ústavního zákona, kterým se mění ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších ústavních zákonů, a ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb. /sněmovní tisk 252/

3. Vládní návrh zákona, kterým se mění zákon č. 159/1999 Sb., o některých podmínkách podnikání a o výkonu některých činností v oblasti cestovního ruchu, ve znění pozdějších předpisů, a další související zákony /sněmovní tisk 761/

5. Vládní návrh zákona, kterým se mění zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů, a některé související zákony /sněmovní tisk 798/

14. Návrh poslanců Tomáše Dubského, Milady Voborské, Martiny Ochodnické, Jiřího Havránka a Jiřího Carbola na vydání zákona, kterým se mění zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů, a další zákony v souvislosti s podporou spolupráce obcí /sněmovní tisk 845/

17. Vládní návrh zákona, kterým se mění zákon č. 243/2000 Sb., o rozpočtovém určení výnosů některých daní územním samosprávným celkům a některým státním fondům (zákon o rozpočtovém určení daní), ve znění pozdějších předpisů / sněmovní tisk 701/

18. Vládní návrh zákona, kterým se mění zákon č. 449/2001 Sb., o myslivosti, ve znění pozdějších předpisů, a další související zákony /sněmovní tisk 732/

22. Vládní návrh zákona, kterým se mění zákon č. 206/2015 Sb., o pyrotechnických výrobcích a zacházení s nimi a o změně některých zákonů (zákon o pyrotechnice), ve znění pozdějších předpisů, a další související zákony /sněmovní tisk 768/

23. Vládní návrh zákona, kterým se mění zákon č. 257/2001 Sb., o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon), ve znění pozdějších předpisů, zákon č. 37/1995 Sb., o neperiodických publikacích, ve znění pozdějších předpisů, a zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon), ve znění pozdějších předpisů / sněmovní tisk 773/

24. Vládní návrh zákona, kterým se mění zákon č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů, a další související zákony /sněmovní tisk 777/

26. Vládní návrh zákona o vstupu a pobytu cizinců (cizinecký zákon) /sněmovní tisk 782/

30. Vládní návrh zákona, kterým se mění zákon č. 477/2001 Sb., o obalech a o změně některých zákonů (zákon o obalech), ve znění pozdějších předpisů, a další související zákony /sněmovní tisk 818/

31. Vládní návrh zákona, kterým se mění zákon č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, ve znění pozdějších předpisů, a další související zákony /sněmovní tisk 849/

79. Návrh Zastupitelstva hlavního města Prahy na vydání zákona, kterým se mění zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů /sněmovní tisk 41/

97. Návrh poslanců Andreje Babiše, Aleše Juchelky, Aleny Schillerové a dalších na vydání zákona, kterým se mění zákon č. 117/1995 Sb., o státní sociální podpoře, ve znění pozdějších předpisů /sněmovní tisk 234/

115. Návrh poslanců Radka Vondráčka, Pavla Blažka, Petra Gazdíka, Lucie Šafránkové, Mariana Jurečky, Vlastimila Válka a dalších na vydání zákona o zemských znacích a vlajkách /sněmovní tisk 400/

160. Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, a další související zákony /sněmovní tisk 728/

elis consulting

8 Na koho dopadne nZKB vycházející z NIS2

Přímý dopad

Regulace NIS2 dopadne přímo na

10 000+ subjektů

z toho na 100% ISP

Tyto subjekty budou zajišťovat kybernetickou bezpečnost ve dvou režimech a podle kritičnosti mohou mít i povinnost řešit tzv. Dodavatelský řetězec.

Nepřímý dopad

Na významnou část ostatních subjektů budou kladeny zvýšené nároky:

- Budou dodávat služby subjektům Strategicky významných služeb
- Budou dodávat služby regulovaným subjektům
- Zákazníci budou vyžadovat aktualizace smluv a definice ochrany proti kybernetickým hrozbám
- Zákazníci budou požadovat vyšší SLA na zajištění služeb

elis consulting

8 Samoidentifikace regulovaného subjektu

Zaměstnanci
Podíváte se počet zaměstnanců všech propojených podniků s ohledem na podíly jednotlivých skutečných vlastníků

Strategická služba
Zjistíte si, zda jste Poskytovatelem Strategicky významné služby a budete tak muset řešit i Dodavatelský řetězec

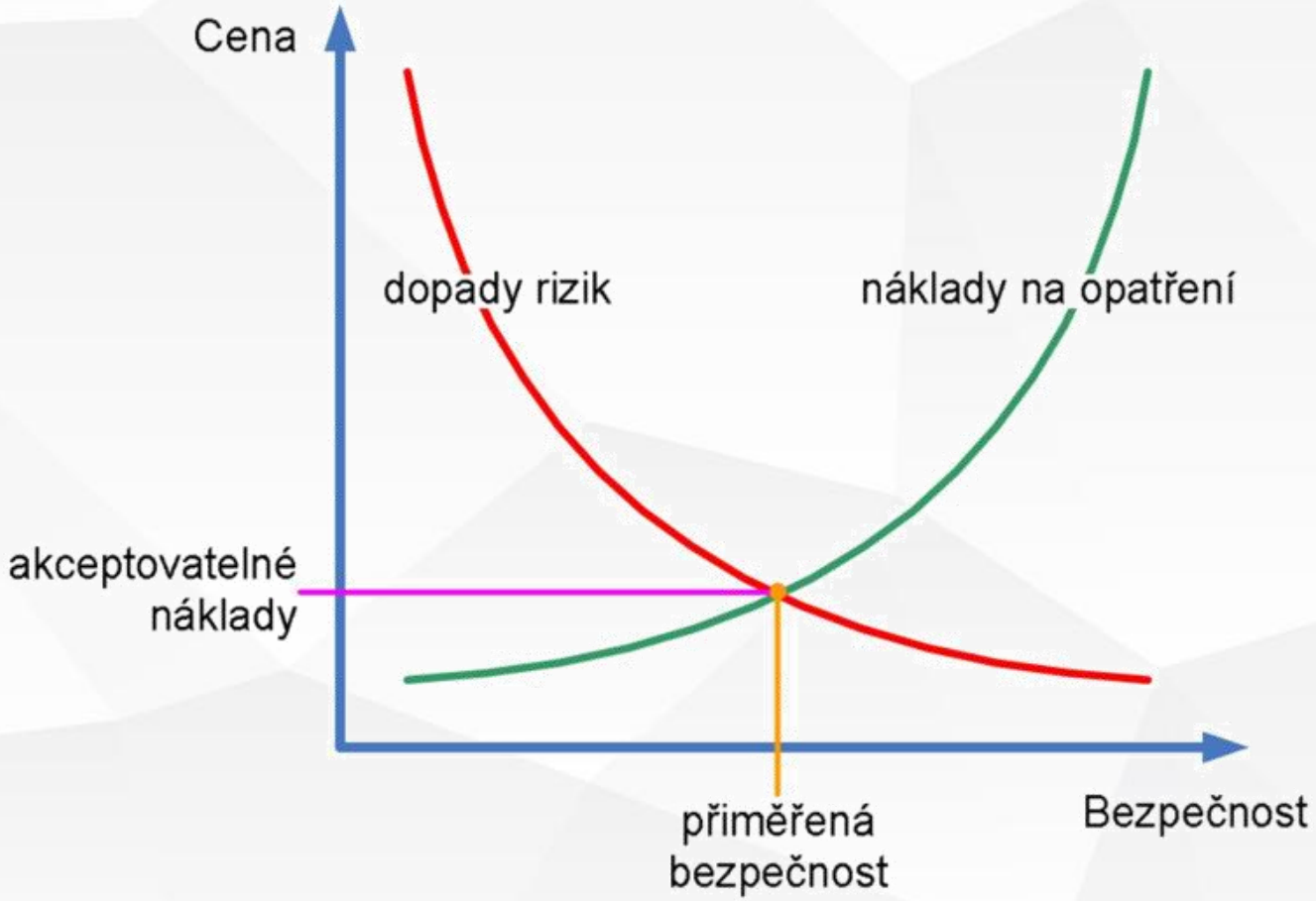
Odvětví
Jako poskytovatelé elektronických komunikací spadáte minimálně do nižšího režimu

Tržba/Rozvaha
Podíváte se na Tržbu a Bilanční sumu roční rozvahy všech propojených podniků, zda za poslední 2 roky převýšila 10+ mil. Eur respektive 50+mil Eur (43 mil. Eur)

Registrace
Zaregistrujete se na Portálu NÚKIB do 30 dnů ode dne, kdy zjistíte, že jste splnili kritéria, lhůta je 90 dní od platnosti nového Zákona o Kybernetické Bezpečnosti (nZKB)

elis consulting

8 Přiměřená bezpečnostní opatření



elis consulting

8 Obsah NIS2 – Zákon nedefinuje technologie a vendory

NIS2 – Článek 21

EUR-Lex
Access to European Union law

2. Opatření uvedená v odstavci 1 jsou založena na přístupu zohledňujícím všechny druhy rizik, jehož cílem je chránit sítě a informační systémy a fyzické prostředí těchto systémů před incidenty, a zahrnují alespoň:

a) politiku analýzy rizik a politiku bezpečnosti informačních systémů;

b) řešení incidentů;

c) řízení kontinuity provozu, jako je například správa zálohování a obnova provozu po havárii, a krizové řízení;

d) bezpečnost dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;

e) zabezpečení pořizování, vývoje a údržby sítí a informačních systémů, včetně zveřejňování zranitelností a jejich řešení;

f) politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik;

g) základní postupy kybernetické hygieny a školení v oblasti kybernetické bezpečnosti;

h) politiky a postupy týkající se používání kryptografie a případně šifrování;

i) bezpečnost lidských zdrojů, postupy kontroly přístupu a správa aktiv;

j) v příslušných případech používání vícefaktorových autentizačních řešení nebo trvalých autentizačních řešení, zabezpečené hlasové, obrazové a textové komunikace a zabezpečených systémů nouzové komunikace v rámci subjektu.

elis consulting

8 Aktuální minimální obhajitelná očekávání NÚKIB v kostce

1. Management digitálních identit, MFA
2. Zero Trust architektura pro firmu, Řízení přístupu, VPN, NDR
3. Ochrana zařízení zaměstnanců, EDR
4. Monitoring, korelace a vyhodnocení logů, XDR, Backup/recovery
5. Definice dodavatelů, aktiv, rizik, dokumentace sítě
6. Interní nebo externí manažer/architekt KB
7. Pravidelné školení managementu a zaměstnanců

elis consulting

8 Služby elis consulting

Služby elis consulting

Díky více než 30 letým zkušenostem umíme pomoci konzultacemi a poradenstvím v oborech TELCO, IT a ICT, a to jak poskytovatelům služeb, tak jejich zákazníkům, kteří požadují tyto služby jako součást dodávky celého telekomunikačního řešení.

Konzultace a poradenství TELCO/IT/ICT

Zpracujeme analýzy ziskovosti, dodavatelských řetězců (hlasové a datové služby, okruhy, konektivita, ústředny, servicedesk, AI/ML, relevance informací na vašem webu atd.

Analýzy a tendry, AI

Poskytovatelům služeb a firmám pomáháme našimi odbornými radami s legislativou týkající se TELCO a ICT služeb, kybernetické bezpečnosti & NIS2, realizujeme kurzy a školení zaměstnanců

Legislativa a NIS2, Kurzy

Profesionalita ^ Odbornost ^ Spolehlivost

elis consulting

elis
consulting

Děkuji za pozornost

„Stay safe and secure“

www.elisconsulting.cz