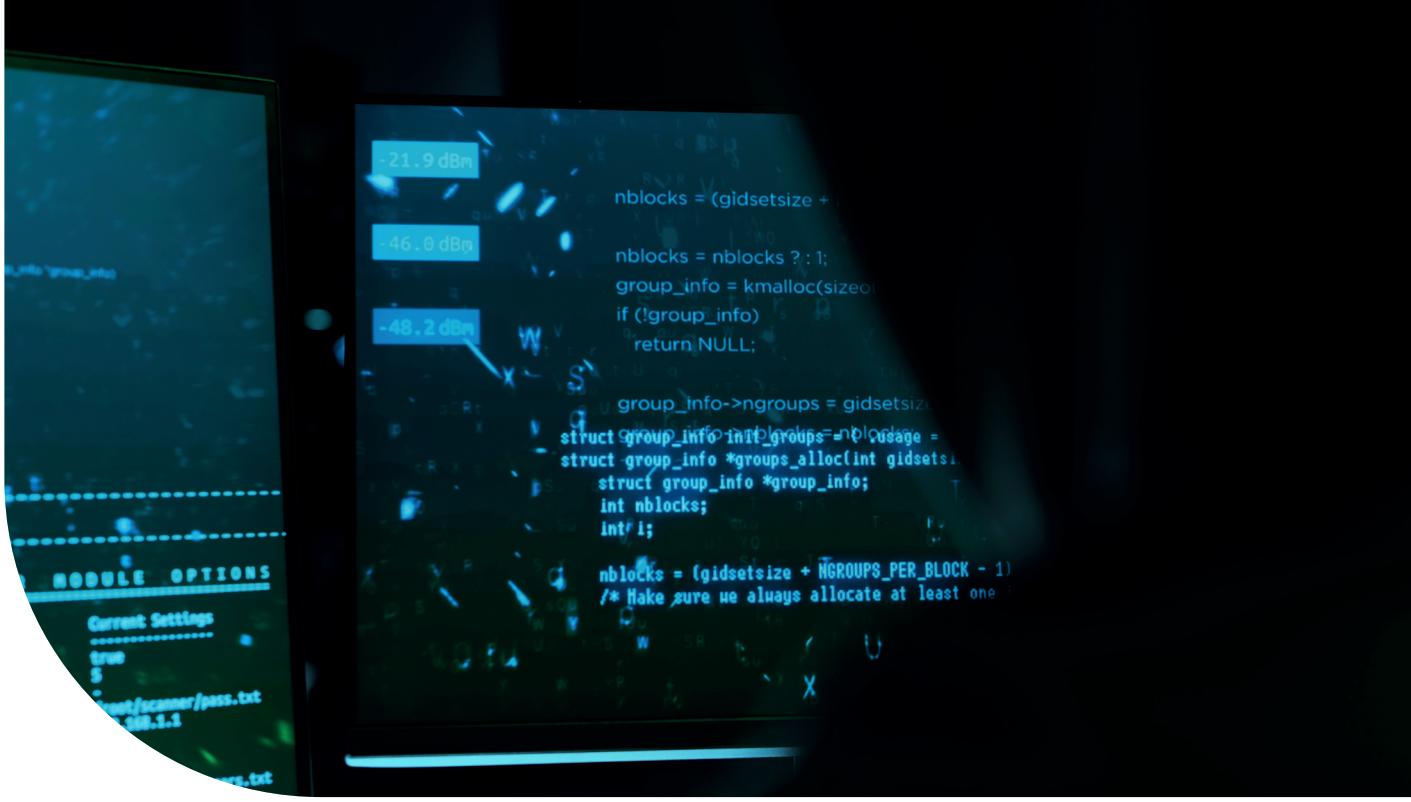
IT KRIZOVÝ PLÁN

Jak se připravit na kybernetický útok

ESET®
Digital Security
Progress. Protected.



Náhle se všechny počítače přepnou do režimu spánku, webové stránky přestanou fungovat a nikdo ze zaměstnanců nemá přístup k síti ani k datům. Celé IT oddělení se náhle zastaví. Jak se ukáže, věci takto zůstanou následující čtyři týdny, protože firma není na tento typ incidentu připravena. Byl by to i váš případ? Pak je tato příručka právě pro vás.

Přestože kybernetických útoků v posledních letech přibývá, je toto téma v mnoha firmách, zejména těch malých a středních, stále podceňováno. Podle průzkumu zpravodajského kanálu CNBCy, 56 % majitelů malých firem v USA v roce 2021 se neobávalo, že by se v příštích 12 měsících mohli stát obětí hackerského útoku, a 24 % z toho nemělo obavy vůbec.

Navíc pouze 28 % malých firem uvedlo, že v případě kybernetického útoku mají plán reakce a 42 % nemá žádný plán.

13%

Takový je podíl menších firem, které školí zaměstnance o kybernetické bezpečnosti. Pouze 19 % z nich testovalo reakce svých zaměstnanců, například pomocí simulace phishingového útoku.

Zdroj: Ipsos MORI a průzkum britského parlamentního výboru pro digitalizaci, kulturu, média a sport, 2021.

Odborníci toto chování hodnotí jako nedbalé. Už není otázkou zda, ale kdy ke kybernetickým útokům dojde. Potvrdil to průzkum, který v roce 2021 zveřejnila německá asociace digitálního průmyslu Bitkom.

9 z 10

Téměř 90 % z 1 000 dotazovaných německých firem z nejrůznějších odvětví uvedlo, že bylo zasaženo kybernetickými útoky. Které typy útoků zmiňovaly tyto firmy nejčastěji?

86%

společností zaznamenalo škody způsobené kybernetickým útokem. V roce 2019 to bylo pouze 70 %.

Zdroj: Bitkom Research, Německo, srovnání průzkumů z let 2019 a 2021.

Začínáme s efektivním krizovým plánem

Odborníci urgentní medicíny označují kritickou fázi při úrazech nebo život ohrožujících onemocněních jako „zlatou hodinu“. Čím rychleji reagujeme, tím větší je šance na úplné zotavení. Profesionální řízení kontinuity provozu je klíčové pro úspěšné zvládnutí této „zlaté hodiny“ ve firemním prostředí. Cílem je zvýšit spolehlivost procesů a rychle a systematicky reagovat na mimořádné události, zejména na hackerské a malwarové útoky.

Krizový plán se často nazývá také „plán reakce na incidenty“. Zahrnuje celý organizační a technický proces reakce na zjištěné nebo předpokládané bezpečnostní incidenty nebo závady v oblasti IT. To zahrnuje i přípravná opatření a postupy. Spektrum možných incidentů sahá od technických problémů a slabých míst až po konkrétní útoky na IT infrastrukturu. Při reakci na IT incidenty je důležité **zohlednit všechny organizační, právní a technické aspekty**.

Šance, že se hackerům útok podaří, jsou velmi vysoké. Samotní kyberzločinci jsou dnes vysoce profesionální. Dnešní hackeři mají k dispozici různé účinné prostředky pro manipulaci a ovládají způsoby, jak po síti šířit vyděračské trojské koně, viry atd. Kybernetický útok navíc **není vždy zaznamenán ihned**, protože nejsou kontrolovány všechny úrovně informačního systému.

Dobrá příprava je při vytváření krizového plánu zásadní. Pokud totiž dojde k nejhoršímu scénáři, je nejdůležitější **reagovat rychle**, co nejrychleji zastavit útok, ochránit uložená data a také co nejdříve obnovit běžný provoz firmy. Proto je třeba stanovit řadu okamžitých opatření: například když se zhroutí celá firemní komunikační síť, webové stránky přestanou být dostupné, nebo se dokonce po útoku zastaví celý výrobní proces.

Jak připravit krizový plán

- **Vypracujte operační krizový plán:** Zaznamenejte všechna nezbytná opatření, která je třeba přijmout v případě mimořádné události. Nejlepší je požádat o radu odborníky.
- **Určete pracovníka odpovědného za IT bezpečnost:** Určete odpovědnou osobu, která se bude zabývat bezpečnostními otázkami ve vaší firmě. Po zavedení GDPR musí podniky s více než 10 zaměstnanci jmenovat pověřence pro ochranu osobních údajů. Pokud spadáte v rámci NIS2 pod nižší režim, je potřeba zajistit osobu, která bude zodpovědná za řízení kybernetické bezpečnosti. Pokud spadáte pod vyšší režim je třeba určit manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a auditora kybernetické bezpečnosti.
- **Zkontrolujte svůj aktuální krizový plán:** Pokud již máte nějaký krizový plán, měli byste ho nechat zkontrolovat odborníky. Měli byste se také ujistit, že je váš krizový plán srozumitelný i pro laiky.
- **Otestujte svůj aktuální krizový plán:** Abyste skutečně věděli, zda plán funguje, musíte ho otestovat předem v praxi.

Kybernetický útok: Co dělat v krizové situaci?

Postupem času způsobují kyberzločinci stále větší škody, pronikají stále hlouběji do IT architektury a získávají velmi citlivá data. Úkolem IT manažerů je proto včas rozpoznat škodlivou činnost a rychle jednat. Jen tak lze minimalizovat škody a vyhnout se úplnému selhání informačního systému. Kromě finančních ztrát by se společnosti měly obávat především poškození pověsti či ztráty důvěry ze strany zákazníků. Co by tedy měly společnosti dělat, když se zločinci zmocní firemních dat?

Kam se obrátit v případě útoku

- Prodejci IT a dodavatelé systémů mají s kybernetickými útoky bohaté zkušenosti a mohou vám poskytnout rychlou a cílenou pomoc.
- Kybernetický útok můžete nahlásit na Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), kde vám odborníci vládního týmu pomohou po technické stránce, včetně poskytnutí rad pro další preventivní opatření. Dojde-li ke zjištění, že některý z incidentů cílí na více subjektů, koordinují společný postup jeho řešení. Incident můžete nahlásit prostřednictvím formuláře nebo e-mailem na cert.incident@nukib.cz.

Nové povinnosti ohledně hlášení bezpečnostních incidentů vyplývají z NIS2/ZKB

Nejpozději do 16. ledna 2025* mají poskytovatelé regulovaných služeb povinnost registrovat se prostřednictvím Portálu NÚKIB. Následně mají 1 rok na to, aby začali hlásit incidenty.

(*V době finalizace této příručky ještě nebyl schválen nový Zákon o kybernetické bezpečnosti, termín se proto může lišit.)

Už víte, jestli patříte mezi poskytovatele regulovaných služeb?

Vyplňte dotazník a zjistěte více podrobností.

Všechny bezpečnostní incidenty, které mají původ v kybernetické prostoru a zároveň u nich nelze vyloučit úmyslné zavinění, případně mají významný dopad (u subjektů ve vyšším režimu stanovuje vyhláška).

- Subjekty spadající do vyššího režimu tyto incidenty hlásí na NÚKIB.
- Subjekty spadající do nižšího režimu tyto incidenty hlásí Národnímu CERT.

Kdy a co přesně hlásit?

1 **Prvotní hlášení:** Bez zbytečného odkladu po zjištění incidentu, nejpozději do 24 hodin je nutné nahlásit identifikační údaje organizace, základní údaje o incidentu, zda byl incident způsoben nezákonným zásahem a zda by mohl mít incident přeshraniční dopad.

Pokud je incident bez „významného dopadu“, tímto krokem hlášení pro organizaci končí.

2 **Oznámení:** Bez zbytečného odkladu nejpozději však do 72 hodin (poskytovatel služeb vytvářejících důvěru do 24 hodin) po zjištění incidentu aktualizace informací z prvotního hlášení.

3 **Průběžná zpráva:** V některých případech jsou podniky vyzvány (NÚKIB nebo Národním CERT) k poslání průběžné zprávy o podstatných změnách stavu zvládání incidentu.

4 **Závěrečná zpráva:** Nejpozději do 30 dnů od oznámení je potřeba poslat podrobný popis incidentu, jeho závažnosti a dopadu, druh hrozby, pravděpodobnou příčinu incidentu, účinná a probíhající opatření ke zmírnění následků a případný přeshraniční dopad incidentu.

Když selže prevence… 9 tipů, které vám pomohou minimalizovat dopad kybernetického útoku

1. Zachovejte klid a jednejte takticky

Pokud bezpečnostní software spustí poplach, je třeba v první řadě zachovat klid. Úspěšný kybernetický útok přichází často nečekaně. Pokud IT oddělení nesleduje všechny úrovně informačního systému, může se škodlivý kód v síti skrývat i několik týdnů, aniž by si jej někdo všiml. Když však k incidentu dojde, je důležité co nejrychleji učinit správná rozhodnutí. Bez krizového plánu s jasně definovanými okamžitými opatřeními může nastat chaos.

2. Určete rozsah útoku

Mnoho IT oddělení ze společností, které se staly obětí malwarových útoků, se při zjišťování důsledků těchto útoků spoléhá spíše na intuici než na hloubkovou analýzu. Je samozřejmě důležité reagovat – ne však na základě domněnek. Pokud má společnost funkční plán pro řešení mimořádných událostí, může IT oddělení rychle najít správné odpovědi na hlavní otázky:

- ☑ Které systémy byly infikovány?
- ☑ Jak k incidentu došlo?
- ☑ Došlo ke ztrátě důležitých dat?
- ☑ Měl útok vliv pouze na jednotlivé komponenty, nebo celou podsíť?
- ☑ Dostaly se informace o zákaznících a zaměstnancích do rukou útočníků?

3. Zajistěte provoz IT

Pokud se interní informace dostanou do rukou neoprávněných osob, je třeba o tom nejprve informovat dotčené zaměstnance a zákazníky. Pokud byly zasaženy útokem IT systémy, měly by být aktivovány záložní systémy a náhradní síťová připojení, protože kybernetický útok by neměl ochromit chod celé firmy. K zajištění tohoto cíle je nutné vypracovat krizový plán, aby byla reakce co nejrychlejší.

4. Izolujte napadené systémy

Infikované IT systémy je třeba izolovat. IT oddělení může odpojit segmenty sítě, ve kterých se nakažené počítače nacházejí, aby se zabránilo šíření útoku v síti. To znamená, že útočníci již nebudou mít k těmto systémům přístup a nemohou „odčerpávat" zpeněžitelná data.

V každém případě by se IT oddělení mělo pokusit dekódovat šifrovanou komunikaci mezi infikovanými IT systémy ve vlastní síti a počítači útočníků. To vám umožní zjistit, zda byly zasaženy i další počítače v síti a jaká firewallová pravidla je třeba použít, aby se zabránilo neoprávněnému přístupu. Tato protiopatření lze realizovat mnohem rychleji a efektivněji, pokud firma používá bezpečnostní řešení.

5. Zajistěte důkazy

Je třeba uchovávat důkazy o incidentech, aby orgány činné v trestním řízení mohly po útoku přijmout náležitá opatření. Komplexní dokumentace vám také může pomoci při uplatnění nároku na náhradu na základě pojistné smlouvy.

6. Odstranění infekce a prevence dalších útoků

Jedním z nejnáročnějších úkolů je vyčistit napadené IT systémy od malwaru a zastavit tak další útoky. Jedním z osvědčených nástrojů je antivirový nebo antimalwarový software, který po instalaci automaticky chrání IT systémy. Je třeba odstranit bezpečnostní mezery, které daný útok umožnily, aby se předešlo dalším útokům stejného druhu.

Abyste měli naprostou jistotu, je vhodné analyzovat datové pakety, které jsou přenášeny po síti. Datový provoz by měl být zkoumán zejména s ohledem na vzorce chování a příkazy, které útočníci dříve používali.

Mezi další bezpečnostní opatření patří kontrola pravidel brány firewall a změna hesel, kterými se zaměstnanci přihlašují do sítě. Za zvážení stojí i hlubší analýza kybernetického útoku, protože v mnoha případech jsou jednotlivé útoky součástí pokročilých přetrvávajících hrozeb (APT). Jedná se o dlouhodobé, komplexní a cílené kybernetické útoky na malé a střední firmy nebo jejich zaměstnance. Pokud se cílem APT skupin stane management, lze předpokládat, že budou následovat další útoky.

7. Legislativa – GDPR, NIS2 a další předpisy

Po kybernetickém útoku vznikají právní problémy – ty by měly být předem vyjasněny. Od zavedení GDPR a s příchodem NIS2 je nutné některé incidenty do určité doby nahlásit úřadům. Povinnost informovat by měla být předem vyjasněna s právním oddělením, aby byla vaše společnost v souladu s právními předpisy a nemusela následně platit další pokuty.

8. Neplaťte vyděračům při ransomwarových útocích

Vyděračský software je oblíbeným prostředkem útoku kyberzločinců. Malware zašifruje data obětí a hackeři pak požadují výkupné za jejich dešifrování. Požadované výkupné nikdy neplaťte, protože nemáte jistotu, že získáte svá data zpět. Navíc byste tím finančně podporovali tento typ kybernetické kriminality. Dáte-li najevo ochotu platit, budou to hackeři brát jako novou výzvu.

9. Z kybernetických útoků se poučte

Je důležité, aby společnosti vyvodily z analýzy útoků správné závěry a přijaly vhodná opatření. Každá nově objevená zranitelnost představuje v konečném důsledku příležitost ke zlepšení ochranných opatření na perimetru firemní sítě a uzavření potenciálních vstupních bodů. Zásadní je také to, aby IT správce pečlivě sledoval všechny úrovně informačního systému. To usnadňuje odhalení kybernetického útoku v rané fázi a nedává narušitelům příležitost proniknout hlouběji a prozkoumat systém před zahájením samotného útoku.

V případě kybernetického útoku se ujistěte, že:

- Útok nemůže způsobit žádné další škody.
- Okamžitá opatření lze provádět nezávisle na nadřízených útvarech nebo na vrcholném vedení, aby se v případě krize neztrácel čas získáváním souhlasu.
- Přihlašovací údaje lze změnit okamžitě. Odcizená hesla, přihlašovací údaje a kompromitované e-mailové účty mohou v budoucnu způsobit další škody. Váš krizový plán by proto měl obsahovat strategii, jak postupovat, když hacker k útoku využije přístupové údaje společnosti.
- Jsou deaktivovány i přístupy pro externí pracovníky a síť je vypnuta. Zejména nespravovaná zařízení hostů představují vysoké riziko průniku škodlivého kódu do systému.
- Nejsou otevřeny žádné e-maily, mobilní zařízení se nepřihlašují do podnikové sítě ani do jiných sítí (např. do sítí zákazníků) a všechna paměťová média připojená k síti, jako jsou USB flash disky, externí disky, kamery atd., jsou odpojena, nepoužívají se, ale zůstávají na pracovišti.

4 další tipy pro větší bezpečnost

Pokud podniknete výše uvedené kroky, jste již na krizi velmi dobře připraveni. Zde jsou další doporučení, která vám pomohou optimalizovat bezpečnost ve vaší firmě:

1. Automatizujte, co se dá

V nejlepším případě by měl být krizový plán z velké části automatizovaný a využívat moderní nástroje. Všechny procesy, které lze provádět automaticky, ulehčí práci IT správci. Mezi tyto činnosti může patřit například automatické odstavení napadených koncových zařízení, kdy jejich firewally odříznou všechna připojení kromě připojení vzdálené správy.

2. Dbejte na logování a dokumentaci

Je také důležité, aby součástí všech akcí, ať už automatických nebo manuálních, bylo důkladné logování a dokumentace jednotlivých kroků. Jedině tak lze zpětně sledovat postup útoku a odpovídajícím způsobem přizpůsobit krizový plán – ať už jde o záplatování možných bezpečnostních chyb nebo o lidské jednání.

3. Pravidelně zálohujte

Bez ohledu na příčinu bezpečnostního incidentu je pro firmy zásadní schopnost co nejrychleji obnovit ztracená kritická obchodní data. Proto je nezbytné začít s pravidelným zálohováním. I zde je dobré automatizovat zálohování dat, protože tím se zajistí soudržnost informací. Kromě toho zajistíte, že zaměstnanci nezapomenou vytvářet zálohy. Záložní kopie by měly být vytvořeny alespoň na dvou externích médiích a je třeba zvážit i šifrovanou verzi zálohy v cloudovém úložišti (s ohledem na ochranu dat je třeba používat evropská úložiště). Systémy zálohování a obnovy je opět třeba pravidelně testovat.

4. Pravidelně revidujte krizový plán

Stejně jako požární cvičení musí být i IT krizový plán pravidelně testován. Není nic fatálnějšího než spoléhat se na plán, který nakonec nefunguje.

Minimalizujte dopady hackerských útoků s ESETem a v souladu s NIS2 a novým Zákonem o kybernetické bezpečnosti

Rozšířená detekce a reakce (ESET Inspect)

Nástroj EDR/XDR umožňuje nepřetržité a komplexní sledování všech aktivit na koncových zařízeních, díky tomu lze podezřelé bezpečnostní incidenty podrobně analyzovat a reagovat na hrozby už v rané fázi. Firmy pomocí technologie EDR/XDR mnohonásobně zvyšují svá bezpečnostní opatření, zejména v případě útoků nultého dne, ransomwaru, cílených útoků (pokročilých přetrvávajících hrozeb) nebo porušení interních firemních předpisů.

Správa zranitelností a záplat (ESET Vulnerability & Patch Management)

Pomáhá organizacím zastavit kybernetické hrozby zneužívající chyby v zastaralých operačních systémech a aplikacích díky další vrstvě zabezpečení, která umožňuje aktivní sledování zranitelností v operačních systémech a automatickému záplatování napříč všemi koncovými body spravovaných prostřednictvím platformy ESET PROTECT.

ESET Threat Intelligence (ETI)

Zpravodajství o hrozbách od odborníků společnosti ESET, jehož součástí je také monitoring aktivních APT skupin. Přináší detailní přehled o taktikách, technikách a postupech útoků (TTPs).

Služby spravované detekce a reakce (ESET MDR)

Služba MDR kombinuje umělou inteligenci a odborné znalosti k detekci hrozeb a rychlé reakce na incidenty, čímž odpadá nutnost mít specializované bezpečnostní odborníky uvnitř organizace. ESET provozuje vlastní globální telemetrickou síť a zpravodajství o hrozbách, které vychází z 35 let zkušeností a využívá data z více než 100 milionů senzorů a 13 výzkumných a vývojových center.

ESET Endpoint Encryption

Každá firma používá pro přenos dat mezi počítači vyměnitelná média. Většina společností však nemá možnost ověřit si, zda údaje zůstávají pouze ve firemních zařízeních. Bezpečné a plně ověřené šifrování zajišťuje ochranu dat vaší organizace v souladu se zákony a předpisy.

Platforma ESET PROTECT

Platforma integruje možnosti prevence, detekce a reakce, zároveň nabízí informace o hrozbách a veškeré služby ESET. Platforma se jednoduše ovládá, je modulární, zároveň přizpůsobitelná a neustále aktualizovaná. Všechny úrovně ochrany ESET používají vícevrstvé technologie, které dalece přesahují možnosti základního antiviru nebo antimalwaru.

ZÁVĚR

Napadení počítačů, serverů nebo mobilních systémů škodlivým softwarem může pro firmy představovat vážnou hrozbu – zejména pokud se interní informace dostanou do rukou útočníků. Takové incidenty však přinášejí dvě důležité informace pro odpovědné osoby: která bezpečnostní IT opatření je třeba optimalizovat a že aktualizovaný plán pro nepředvídané události může minimalizovat škody.

Technologie pomáhají měnit svět k lepšímu. ESET je tady, aby je chránil.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích. ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Další informace naleznete na eset.cz nebo nás sledujte na sítích LinkedIn, Facebook, and X.

Domácnosti

Firmy

Stát

ESET V ČÍSLECH

1mld+
chráněných uživatelů na internetu

400k+
firemních zákazníků

200
zemí a teritorií

13
vývojových center