HOSPODÁŘSKÉ NOVINY

SPECIÁLNÍ PŘÍLOHA

# KYBERNETICKÁ BEZPEČNOST

**Zrychlení na minuty**

Kybernetická válka v éře AI se zrychlila. Firmy si musí připustit, že se útok může stát, a investovat, říká v rozhovoru Václav Svátek.

**Digitální štít Evropy**

Evropská unie spouští další vlnu kyberbezpečnostní regulace. Pozornost od institucí obrací k samotným produktům.

▸Rozhovor

**Adam Mašek**
adam.masek@economia.cz

# Kybernetická válka v éře AI se zrychlila na minuty. Firmy ale stále šetří na základech

Trh s IT infrastrukturou prožívá největší otřes za poslední dekády. Zatímco útočníci díky umělé inteligenci zkrátili přípravu útoků z dnů na minuty, české firmy čelí extrémnímu zdražování hardwaru i cloudových služeb. „To, co dříve v serveru stálo milion, dnes vyjde na šest milionů. Éra levného digitálního prostoru končí a s ní i falešný pocit bezpečí," říká v rozhovoru pro HN Václav Svátek, generální ředitel společnosti ČMIS, jež se specializuje na dodávání cloudových služeb a kybernetickou bezpečnost.

**V rámci vaší „ransomware pohotovosti" řešíte případy firem, které se staly obětí kyberútoku. Jaká je aktuální situace na českém trhu?**
V průměru řešíme zhruba čtyři závažné případy měsíčně. Nejde jen o malé firmy s deseti počítači. Obětmi jsou i velké společnosti s miliardovými obraty, u kterých byste čekali špičkové zabezpečení. Bohužel stále platí, že velikost firmy nerovná se automaticky její bezpečnost. Vidíme útoky, které jsou čistě ekonomické, kde jde o výkupné, jež se vyplácí v kryptoměnách, ale i sofistikované operace sponzorované cizími vládami. Jejich cílem je primárně špionáž a získání přístupu k infrastruktuře. To, co se zásadně změnilo, je rychlost. Díky umělé inteligenci trvá útočníkům nalezení zranitelnosti a provedení útoku minuty, zatímco dříve to byly hodiny nebo dny.

**Kudy se útočníci do českých firem nejčastěji dostávají?**
Vektor útoku je v 70 až 80 procentech případů stejný: nedostatečně zabezpečený přístup do firemní sítě přes VPN bez dvoufaktorového ověřování. Pro mě je to nepochopitelné, protože taková ochrana stojí jednotky eur měsíčně, ale firmy to stále podceňují. Útočník se dostane do počítače zaměstnance, který doma nakupuje na pochybných e-shopech nebo navštěvuje rizikové stránky, nainstaluje tam malware a pak už jen čeká, až se uživatel připojí k firemním zdrojům. Jakmile je útočník uvnitř perimetru, AI mu pomůže bleskově oskenovat síť, najít staré, nezáplatované systémy a celou infrastrukturu zašifrovat.

**Hodně se mluví o nové evropské regulaci NIS2, která je v Česku implementována skrze nový zákon o kybernetické bezpečnosti. Mohou povinnosti, které z něj na firmy přímo dopadají, pomoci?**
NIS2 je krok správným směrem, ale realita v komerčním sektoru je rozpačitá. Vidím tam rozdělení na dvě skupiny: zhruba pětina firem to vzala vážně a skutečně buduje procesy. Zbylých 80 procent hledá jen způsob, jak v uvozovkách vyplnit šanon, najmout si formálního manažera bezpečnosti a doufat, že je nikdo nebude kontrolovat. Často narážíme na odpor i u samotných IT administrátorů. Bezpečnost totiž z principu komplikuje práci – musíte se vícekrát identifikovat, máte zamčené dveře do některých procesů, systémů a podobně. Lidé si práci rádi zjednodušují, čímž ale vytvářejí kritické díry v systému.

**Co byste poradil manažerům, aby jejich firma takový útok přežila?**
Klíčové je připustit si, že se to může stát. Musíte mít záchranný plán, podobně jako víte, že máte v autě lékárničku a voláte 155. Naprostá většina firem přežije dvoudenní výpadek, ale nikdo nepřežije kompletní ztrátu dat budovaných dvacet let. Manažerským selháním není to, že vás napadnou, ale to, že nejste schopni obnovit provoz do 24 hodin. Máme případy státních podniků nebo nemocnic, které se po útoku vracely do „pravěku" a pracovaly s papírem a tužkou celé měsíce, protože neměly funkční disaster recovery plán.

**Zmínil jste, že kyberbezpečnost dnes naráží i na ekonomickou realitu trhu s hardwarem. Jak vážná je situace?**
Je to systémová krize. Za posledních osm měsíců došlo k šílenému zdražení klíčových komponent. Paměti RAM zdražily desetinásobně – modul, který stál 15 tisíc, dnes stojí 150 tisíc korun. U NVMe datových disků jsme na šestinásobku ceny. Celkově se vybavený server dnes prodává za čtyř- až šestinásobek původní ceny. To, co dříve stálo 500 tisíc korun, dnes vyjde na čtyři miliony korun. A nejde jen o cenu, ale i o dostupnost. Na servery, které dříve byly u nás v datacentru do 14 dnů, se dnes čeká i čtyři měsíce.

**Co je hlavní příčinou tohoto stavu?**
Tentokrát to není o přerušených lodních trasách jako za covidu, ale o strategickém rozhodnutí výrobců. Giganty jako Google, Microsoft či Meta si zarezervovaly výrobní kapacity světových továren Samsungu, Micronu a SK Hynix na mnoho měsíců dopředu. Výrobci raději produkují speciální paměti pro AI akcelerátory (specializované a velmi výkonné čipy určené výhradně pro složité výpočty AI – pozn. red.), na kterých mají obrovské marže, a omezují linky na standardní paměti pro běžné servery. Tento stav bude podle všech indicií trvat minimálně další rok a půl.

**Klíčové je připustit si, že se útok může stát.** *Musíte mít záchranný plán, podobně jako víte, že máte v autě lékárničku a voláte 155.* **Foto: Libor Fojtík**

**Jak se tento nedostatek promítne do cen cloudových služeb?**
Cloudoví obři jako Azure, AWS či Google už nenápadně zdražují. Přestávají podporovat starší, levnější instance, zdražují ukládání dat a síťový provoz. Největší riziko ale vidím u takzvaných spotových instancí, což jsou virtuální servery se slevou až 90 procent, které ale poskytovatel může kdykoliv vypnout. V momentě, kdy je hardwaru málo, budou tyto instance mnohem méně dostupné a mnohem častěji ukončované. Firmy, které na nich dnes staví svůj provoz, mohou čelit situaci, kdy se jim cloud skokově zdraží osminásobně, protože budou muset přejít na garantovaný výkon.

**Jak na to reagujete vy v ČMIS? Dá se proti takovému vývoji vůbec pojistit?**
My jsme měli štěstí a trochu jsme spekulovali. Už loni v létě jsme dostávali varování od výrobců, že se bude zdražovat. Na poslední chvíli, koncem roku, jsme tedy nakoupili paměti a disky asi za 61 milionů korun ještě za relativně nízké ceny. Díky tomu dnes máme v datacentru volné kapacity – zhruba deset terabajtů operační paměti a petabajty diskového prostoru. Ty můžeme zákazníkům nabídnout za výrazně lepších podmínek, než jaké budou mít globální cloudy od letošního září.

**Máte pocit, že se investice do AI, které tento nedostatek způsobily, big tech firmám vyplatí?**
Osobně očekávám jisté vystřízlivění. Dnes na jeden dolar utracený zákazníkem za AI připadá sedm dolarů nákladů na straně poskytovatele, což je neudržitelné. Už nyní vidíme omezování předplatných a zavádění limitů na tokeny. Brzy se může ukázat, že provoz některých AI modelů je dražší než práce kvalifikovaného člověka. Do té doby ale bude hardware vzácnou komoditou. Firmy musí revidovat své rozpočty a uvědomit si, že levné IT bylo anomálií, která končí.

**Co to tedy pro českého podnikatele vlastně znamená?**
Že by bylo bláhové čekat, že hardware nebo cloud zlevní. Normalizace trhu přijde nejdříve v roce 2028. Pokud odkládáte investice do bezpečnosti nebo obnovy serverů, riskujete, že se v případě incidentu nedoplatíte nebo na hardware budete čekat čtvrt roku. A to může být pro firmu likvidační. Kyberbezpečnost už není technický problém, je to klíčová manažerská disciplína pro přežití firmy.

## Václav Svátek (45 let)

- Vystudoval obor Teorie a technika jaderných reaktorů na ČVUT.
- Společnost Českomoravské informační systémy založil u ž v roce 2004, od roku 2012 se firma jmenuje zkráceně ČMIS.
- Specializuje se na dodávky služeb v oblasti IT a cloudu. Pro třetí strany konzultuje také kyberbezpečnost a provádí penetrační testy či bezpečnostní audity.
- Součástí provozu je i takzvaná kybernetická ambulance, která firmám pomáhá okamžitě řešit problémy spojené s kyberútoky.
- V roce 2013 založil další společnost AppOnFly, cloudovou platformu, která uživatelům umožňuje vzdáleně streamovat virtuální počítače (Windows VPS) přímo ve webovém prohlížeči.

**Příloha: Kybernetická bezpečnost**
• **Ředitel speciálních projektů** Aleš Mohout • **Editor** Ján Chovanec (jan.chovanec@economia.cz) • **Grafika a zlom** Vizuální studio Economia • **Obcod a inzerce** Daniel Hort (daniel.hort@economia.cz)
**Partner vydání:** 4CYBER

Inzerce

# Red teaming otestuje vaši firmu dřív, než to udělají hackeři

**Většina českých firem dnes ví, že má dělat penetrační testy. Málokterá ale ví, čím se liší od skenu zranitelností a ještě méně z nich tuší, kdy je čas posunout se k red teamingu. Pro majitele a jednatele jde přitom o úplně jinou otázku než „kolik máme děr v síti“. Jde o to, zda si firmy dokážou všimnout, že je někdo uvnitř.**

## Jaký je rozdíl mezi skenem zranitelností, penetračním testem a red teamingem?

Představte si, že chcete ověřit, jak je zabezpečená vaše centrála. Nejlevnější variantou je obejít budovu a zaznamenat, které dveře jsou zamčené. To je v IT sken zranitelností. Automatický nástroj proběhne přes systémy a vrátí seznam toho, co někdo zapomněl zamknout. Chybějící aktualizace, otevřené porty, zranitelné verze služeb. Užitečné, levné a mělo by se to dělat průběžně.

Druhá úroveň je penetrační test. Najmete profesionála, který má za úkol zkusit ty zámky překonat a navíc se podívat na okna a sklep. V IT terminologii to znamená, že tester se podívá na dohodnutý systém (webovou aplikaci, vnitřní síť, mobilní aplikaci) a snaží se v něm najít a zneužít zranitelnosti. Výsledkem je seznam zjištěných chyb seřazený podle závažnosti a doporučení, jak je opravit. Penetrační test je dnes standard a nový český zákon o kybernetické bezpečnosti, účinný od 1. listopadu 2025, ho v některých režimech vyloženě počítá mezi opatření, která musí firmy v regulovaných odvětvích zavést.

A pak je tu třetí úroveň red teaming. Tady otázkou není „kde máme díry?“, ale „jak dlouho útočníkovi trvá, než nám něco zásadního vezme, a všimneme si toho vůbec?“.

## Jak red team funguje?

Red team je skupina lidí, která dostane za cíl například „získat přístup k zákaznické databázi“ nebo „dostat se do účetního systému s právy vedoucího finančního oddělení“ a může si k tomu zvolit jakoukoli cestu. Pošle zaměstnancům phishing, zavolá na helpdesk, že je nový kolega a potřebuje odemknout účet nebo vejde s návštěvníky do budovy, nasadí si visačku vyrobenou podle fotky z LinkedInu a zapojí malou krabičku do zásuvky v zasedačce. Red team tedy zkouší různé cesty od virtuálních až po ty fyzické, aby se dostal ke svému cíli, stejně jako útočník. Důležité zároveň je, že ve firmě o této simulaci skoro nikdo neví.

## Jak dlouho red teaming trvá?

Čtyři týdny až měsíce, záleží na rozsahu simulace. Pokud totiž musíte cestovat např. po výrobních závodech, není to cesta na jeden den, ale v dané lokalitě strávíte minimálně týden. Někteří klienti chtějí pouze virtuální red teaming, což zkracuje dobu testu.

## Pro koho má red teaming smysl? Pro malou firmu o 30 lidech to asi nebude.

Říká se, že red teaming má smysl pro větší firmy, které už mají hotovou základní hygienu. Například pravidelně testují svoje systémy skenem zranitelností a penetračními testy. Máme ale i výjimky menších startupů s unikátním know-how, kdy se majitelé bojí o svá data a chtějí otestovat, co by dokázal odcizit útočník nebo například konkurence.

## Co když se něco pokazí? Například někdo zavolá policii, nebo vás zastaví ochranka?

Na tuto situaci je samozřejmě potřeba myslet dopředu. Naši testeři jezdí vždy s tzv. „get-out-of-jail letter“, což je dokument podepsaný klientem. V tomto dokumentu je specifikován rozsah testu, kontakty na osoby, které vědí, že testování probíhá, a jejich podpisy.

## Co je výsledkem red teamingu?

Hlavně společný debrief. Není to jen technická zpráva. Sedneme si s vedením společnosti, IT a ostrahou objektu k jednomu stolu a projdeme si celou časovou osu. V 7:42 vešel náš red teamer hlavním vchodem. V 8:11 zapojil zařízení v zasedačce 2A. V 9:30 jsme byli ve vaší síti. V 14:24 tento člověk klikl na phishing a díky tomu jsme se dostali na tato místa. Tady jste si nás všimli a zastavili, tady ne. Projdeme si celý souběh událostí, který vedl k našemu cíli, s doporučeními, co by šlo vylepšit.

## Kolik red teaming stojí?

Vždy záleží na několika faktorech. Kolik má firma poboček a zaměstnanců. Zda klient požaduje kompletní red teaming i s fyzickou částí, nebo jen virtuální red team bez toho, abychom vstoupili za brány společnosti. To vše otevírá, případně zavírá útočné vektory. Vždy si po úvodní bezplatné konzultaci s klientem necháme 14 dní na rychlý OSINT. Zjistíme co nejvíce informací z veřejných zdrojů, vymyslíme vektory útoku, vypočítáme, kolik lidí budeme do teamu potřebovat a také časovou náročnost. Až potom jsme schopni připravit nabídku, která začíná od půl milionu korun až po nižší miliony. Red teaming je pro firmy, které kybernetickou bezpečnost chtějí brát vážně. Je to jediný způsob, jak otestovat svoji bezpečnost dřív, než to udělají hackeři.

**Patrik Žák –** etický hacker, red teamer a spoluzakladatel společnosti SYSNETSHIELD

▸Bezpečnost firem

# Kyberútok už nevede přes vaši firmu. Přichází přes dodavatele

**Ján Chovanec**
jan.chovanec@economia.cz

Firmy v posledních letech výrazně posílily vlastní kybernetickou bezpečnost. Investují do technologií, zavádějí vícefaktorové ověřování, školí zaměstnance a budují bezpečnostní týmy. Přesto počet úspěšných útoků neklesá. Útočníci totiž změnili strategii. Místo přímého útoku na dobře chráněnou organizaci stále častěji hledají nejslabší článek v jejím okolí – dodavatele.

Takzvané supply chain útoky, tedy útoky skrze dodavatelský řetězec, patří dnes mezi nejrychleji rostoucí hrozby. Princip je jednoduchý: kompromitovat menší firmu nebo technologického partnera bývá výrazně snazší než proniknout přímo do velké společnosti. Jakmile se to podaří, útočník získává nepřímý přístup do systémů všech zákazníků napadeného dodavatele. Jeden incident se tak může velmi rychle proměnit v problém pro desítky dalších firem.

Digitální ekonomika přitom vytvořila prostředí, ve kterém jsou firmy propojené více než kdy dříve. Využívají cloudové služby, externí vývojáře, open-source knihovny i specializované SaaS platformy. Jediný produkt tak dnes často obsahuje desítky až stovky komponent od různých subjektů. Každý z nich představuje potenciální vstupní bod pro útok. Bezpečnost firmy se tak fakticky posouvá mimo její vlastní hranice.

### Útok přichází „legální cestou“

Typickým scénářem je kompromitace softwarové aktualizace. Firma si stáhne legitimní update od důvěryhodného dodavatele, který byl mezitím napaden. Aktualizace obsahuje škodlivý kód, který se následně automaticky rozšíří do všech systémů, kde je software nasazen. Útok tak proběhne bez nutnosti prolomit zabezpečení cílové organizace – využije důvěru, na které je digitální ekosystém postaven.

Podobně fungují i útoky přes vzdálený přístup dodavatelů do firemních systémů. Externí IT partner, servisní firma nebo vývojář má často oprávnění, která by interní zaměstnanec získával jen obtížně. Pokud je tento přístup špatně zabezpečený, stává se ideální vstupní branou. Útočník se tak dostává „dovnitř“ bez nutnosti překonávat perimetr firmy.

### Regulace tlačí firmy k odpovědnosti za celý řetězec

Právě na tuto změnu reaguje i evropská legislativa. Směrnice NIS2, která výrazně rozšiřuje okruh regulovaných subjektů, ukládá firmám povinnost řídit rizika v dodavatelském řetězci jako nedílnou součást kybernetické bezpečnosti. Nejde přitom jen o technická opatření, ale i o procesy výběru a kontroly partnerů, smluvní nastavení odpovědností nebo průběžné hodnocení jejich bezpečnostní úrovně.

Firmy tak budou muset systematicky řešit otázky, které dosud stály spíše na okraji: jaké bezpečnostní standardy musí dodavatel splňovat, jakým způsobem se ověřuje jejich dodržování, kdo nese odpovědnost v případě incidentu nebo jak rychle je partner schopen reagovat na zranitelnost. Bezpečnost se tak dostává přímo do obchodních vztahů a smluv.

Nařízení Cyber Resilience Act tuto logiku doplňuje z druhé strany. Zaměřuje se na samotné digitální produkty a komponenty, ze kterých se systémy skládají. Výrobci budou muset například evidovat takzvaný Software Bill of Materials, tedy detailní seznam použitých knihoven a softwarových prvků. Cílem je umožnit rychlou identifikaci zranitelností napříč celým dodavatelským řetězcem a zamezit situaci, kdy firma ani neví, že používá kompromitovanou komponentu.

### Bezpečnost se přesouvá z IT do byznysu

Z papíru do praxe je ale cesta složitá. Mnoho firem dnes nemá přesný přehled o tom, jaké komponenty jejich systémy obsahují a odkud pocházejí. Moderní software vzniká jako kombinace vlastního vývoje a externích zdrojů, které se průběžně aktualizují. Zmapování celého ekosystému tak představuje náročný a dlouhodobý proces, který vyžaduje nejen technologické nástroje, ale i změnu interních procesů.

Další výzvou je řízení samotných dodavatelů. Velké korporace začínají zavádět bezpečnostní audity a přenášet odpovědnost do smluv, menší firmy ale často nemají kapacity ani vyjednávací sílu. V praxi tak platí, že úroveň zabezpečení celého řetězce určuje jeho nejslabší článek – a tím bývá často právě menší partner, který bezpečnost řeší jen okrajově.

Pro management to znamená zásadní posun. Kyberbezpečnost už nelze chápat jako izolovanou funkci IT oddělení. Stává se součástí nákupu, řízení dodavatelů i strategického rozhodování. Výběr partnera tak není jen otázkou ceny a kvality služby, ale i jeho schopnosti odolat kybernetickým hrozbám.

Roste také tlak na transparentnost. Zákazníci i regulátoři budou stále častěji požadovat důkazy o tom, že firma má svůj dodavatelský řetězec pod kontrolou. Nestačí deklarovat bezpečnost, bude nutné ji prokazovat – a to nejen u sebe, ale i u všech klíčových partnerů.

Útočníci si totiž dobře uvědomují, že nejsnazší cesta nevede přes hlavní bránu, ale přes zadní vchod. A v digitální ekonomice je tímto vchodem téměř vždy někdo jiný.

**Softwarové aktualizace jako riziko.** *Pokud je tento přístup špatně zabezpečený, stává se ideální vstupní branou. Útočník se tak dostává „dovnitř“ bez nutnosti překonávat perimetr firmy.* **Foto: Shutterstock**

▸Komentář

# AI mění pravidla transakcí: Proč software za miliony ztrácí hodnotu

**Jakub Dohnal**
autori@economia.cz

Nejsem ajťák. Jsem transakční právník, kterého baví reálný byznys a převody podílů. Z této perspektivy jasně vidím, že překotný nástup umělé inteligence zcela zásadně mění dynamiku fúzí a akvizic. Kyberbezpečnost a softwarové právo už zkrátka nejsou jen formální položkou v checklistu na konci prověrky, ale klíčovým faktorem, který určuje finální cenu celé transakce.

Pěkně to ilustruje příklad z praxe. Když dnes prodáváte e-shop a investorovi argumentujete tím, že máte ve vlastním softwaru nainvestováno pět milionů korun z předloňska, dotyčný se jen pousměje. To, co se dříve kódovalo dlouhé měsíce, dnes s pomocí AI poskládáte za zlomkovou cenu. Hodnota staršího softwaru letí dolů. Transakční prověrky jsou sice díky novým technologiím v mnoha ohledech jednodušší, ale rizika, která odkrývají, jsou nesrovnatelně větší.

Investory dnes extrémně zajímá, zda dravá implementace AI neproběhla na úkor bezpečnosti. Pokud vaši lidé v honbě za rychlostí sypali interní know-how, marže nebo klientská data do veřejných modelů, doslova jste vytunelovali hodnotu vlastní firmy. V éře nastupujících regulací NIS2 a AI Actu už nejde o teoretické hrozby, ale o tvrdá transakční kritéria. Na konci dne je byznys pořád o tom samém – o tom, kdo dává na stůl finální razítko a nese kůži na trh. Algoritmus za vás odpovědnost neponese.

**Nástroje pro ochranu hodnoty firmy.** *Správně ošetřené IT právo tu není od toho, aby inovace dusilo, ale aby fungovalo jako transakční štít.* **Foto: Jan Kolman**

Kyberbezpečnost proto vnímám jako nejlepší nástroj pro ochranu hodnoty firmy. Správně ošetřené IT právo tu není od toho, aby inovace dusilo, ale aby fungovalo jako transakční štít. Pokud chcete společnost jednou se ziskem prodat nebo do ní pustit strategického partnera, dravost bez bezpečnosti není pokrok, ale hazard, který vám při příštím prodeji nikdo neodpustí.

JUDr. Jakub Dohnal, Ph.D.
řídící partner advokátní kanceláře
ARROWS

▸4cyber

**Marcela Štefcová**
marcela.stevcova@economia.cz

# Jeden klik může položit i stoletou firmu – tradiční školení kyberbezpečnosti selhávají

Kybernetické útoky se stále více přesouvají od technické infrastruktury k lidem. Phishing, smishing, vishing a podvody generované umělou inteligencí jsou dnes přesvědčivější než kdykoli dřív. „Můžete mít investované obrovské prostředky do interní bezpečnosti, ale když vám jeden zaměstnanec klikne na podvojný e-mail nebo zadá osobní údaje, problém je na světě," upozorňují zakladatelé firmy 4cyber, Lukáš Pirkl, David Pirkl a Jiří Sommer. V dnešní době už nestačí zaměstnance jednou za rok plošně školit, firmy musí cílit na měření a řízení lidského rizika. Jaká rizika přináší slepá důvěra lidí v AI nástroje a jak se efektivně bránit hrozbám, které míří na tu nejzranitelnější část každé organizace?

**Kvůli kybernetické bezpečnosti firmy investují velké částky do firewallů a zabezpečení, přesto počty úspěšných útoků rostou. Co přesně se aktuálně děje?**
**David Pirkl (DV):** Útoky se stále více přesouvají na lidi. Díky pokročilým technologiím a umělé inteligenci je dnes obranná infrastruktura firem mnohem sofistikovanější. Pro hackery je tak logicky daleko složitější proniknout přes kvalitně zabezpečenou infrastrukturu než oklamat zaměstnance. Proto se vektor útoků přesouvá do sociálního inženýrství, phishingu a lidských chyb. Lidé jsou sami sobě největším nepřítelem – na sociálních sítích veřejně sdílejí množství informací, od jmen domácích mazlíčků přes data výročí až po oblíbené značky.

Útočníkovi pak stačí nasadit automatizovaný skript, stáhnout si pět takových detailů, vložit je do kombinátoru a vygenerovat dvacet vysoce pravděpodobných hesel. Pokud se podíváme na bankovní sektor v Česku, tak za první kvartál loňského roku přišli lidé o 397 milionů korun. Za letošní první kvartál už se ale bavíme o 800 milionech korun. Firmy si začínají uvědomovat tato rizika více než dřív, ale stále existuje propast mezi tím, co říkají, a tím, co skutečně dělají.

**Největším rizikem je tedy zaměstnanec? Firmy ale přece tvrdí, že své lidi alespoň jednou ročně školí…**
**Lukáš Pirkl (LP):** Pouhé jednorázové plošné proškolení zaměstnanců je naprosto neefektivní, protože se de facto jedná jen o splnění formální povinnosti a získání podpisu. Externí IT školitel dvě hodiny mluví ke stovce lidí, kteří často moc neposlouchají, a na konci jen podepíší prezenční listinu. Vy jako zaměstnavatel nevíte, kdo dával pozor a co si z teoretického výkladu odnesl do praxe. Nemáte žádnou zpětnou vazbu, žádná data.

**A jak mění umělá inteligence bezpečnostní situaci ve firmách?**
**DV:** Používání umělé inteligence je dnes klíčová věc, ale zároveň obrovská hrozba. Využívání AI se ve firmách šíří mnohem rychleji než bezpečnostní pravidla. Ve snaze urychlit práci zaměstnanci běžně nahrávají osobní údaje, obchodní data a smlouvy, aby jim umělá inteligence udělala výtah nebo analýzu, a vůbec si neuvědomují, že tímto krokem odevzdávají citlivé údaje do prostoru. Tento neutěšený stav má řešit evropské nařízení AI Act, který firmám ukládá povinnost zajistit AI gramotnost zaměstnanců. Společnosti tak budou brzy nuceny prokazovat, že jejich lidé bezpečnému využívání AI rozumí, znají její limity a chápou rizika. Podobně jako v případě zákona o kybernetické bezpečnosti a směrnice NIS2 ale platí, že tyto zákony nemají firmy šikanovat. Dávají jasná doporučení, že musíte mít interní směrnice a prokazatelně zaměstnance vzdělávat. Problém je, že bez reálných dat z analýz a testování nemůžete lidské riziko efektivně řídit.

**Jak má tedy postupovat firma, která se chce skutečně zabezpečit, ne pouze splnit formální požadavky?**
**Jiří Sommer (JS):** Jsou dvě roviny. Z pohledu technické infrastruktury firmy a z pohledu lidí, tedy takzvaný Human Risk Management. Za prvé, firma musí vědět, co chrání – začít auditem a analýzou, identifikovat citlivá data, nastavit interní pravidla, provést analýzu z pohledu NIS2. Nejhorší, co může firma udělat, je bez jakýchkoliv podkladů a dat slepě nakupovat drahá softwarová řešení, která jí nakonec k ničemu nebudou.

Za druhé, musí řídit lidské riziko. Nejen vzdělávat, ale i testovat zaměstnance, měřit výsledky, cíleně dovzdělávat. Většina firem dnes vyhledá jednu firmu na školení a jinou na phishingové testy. Nemá to propojené, nedokáže řídit celý cyklus. My jsme první platforma na českém trhu, která tyto věci integruje: e-learning, phishingové a smishingové simulace, bezpečné používání AI, reporting a auditní stopa – vše z jednoho místa.

**V čem konkrétně je tedy platforma 4CyberCity jiná než to, co si firmy běžně kupují? Jak vypadá z pohledu školeného zaměstnance i správce?**
**JS:** Zásadní rozdíl je v centralizaci a automatizaci. Vše propojujeme do jednoho intuitivního nástroje. Stručně řečeno zaměstnance moderní, zábavnou a gamifikovanou formou proškolíme a rovnou je v reálné, byť bezpečné situaci otestujeme simulovaným útokem. Pošleme jim podvržený phishingový e-mail nebo SMS, tedy smishing, a exaktně měříme, jak zareagují. Zda na podvodný odkaz kliknou, zadají své přihlašovací údaje. Cílem přitom rozhodně není lidi šikanovat a rozdávat pokuty. Chceme hravou a neagresivní formou ukázat: tady jsi udělal chybu, tohle sis měl ověřit a pojďme se naučit, jak to poznat příště.

Prakticky se zaměstnanec přihlásí a vidí svá témata, která odpovídají jeho pozici ve firmě, tedy personalizovaná. Každé obsahuje krátké video do dvou minut, studijní text a tři příběhové scénáře. Těmi ho provází virtuální hacker, který mu vysvětluje, jak by využil toho, co udělal špatně. Je to interaktivní, zvladatelné i v mobilu. Na konci pak čeká krátký test a zaměstnanec získá certifikát.

Pro správce je k dispozici dashboard, kde vidí, kdo se přihlásil, co nastudoval, jak mu to šlo. Může na pár kliknutí vytvořit phishingovou kampaň, zacílit ji na konkrétní tým a pak vidí, kdo klikl, kdo vyplnil osobní údaje. Výsledky jsou propojené s dalším vzděláváním. Když někdo klikne, okamžitě dostane zpětnou vazbu – přesměrování na interní směrnice firmy nebo na video, které mu vysvětlí, že právě klikl na cvičný phishing, a vysvětlí mu, co přesně bylo na daném e-mailu podezřelé. Když to zaměstnanec zažije opakovaně a třikrát za sebou na něj takto vyskočí varování, psychologie zafunguje a příště si dá velký pozor.

A systém navíc umožňuje cílené doškolování. Už neškolíme účetní, adminy a manažery stejným plošným obsahem. Každý má jiný přístup k datům a dostává takový obsah, který odpovídá jeho skutečným slabinám a reálnému riziku. Z toho pak vzniká naprosto detailní a exaktní auditní stopa, která je zásadní nejen pro bezpečnost, ale i pro management při dokládání plnění legislativy.

**A tato vaše platforma je již dokončená? Kde se 4cyber vidí za pět let?**
**LP:** Naši platformu 4CyberCity dál rozšiřujeme směrem k bezpečnému používání umělé inteligence ve firmách. Aktuálně dokončujeme moduly zaměřené na AI gramotnost zaměstnanců a bezpečnou práci s AI nástroji. Dalším krokem je posun od řízení lidského rizika k širšímu řízení firemní compliance a bezpečnostního rizika napříč celou organizací. Chceme vytvořit platformu, do které firma nahraje své dokumenty, interní směrnice a bezpečnostní politiky, napojí používané AI nástroje a získá automatizovanou analýzu, nakolik splňuje požadavky NIS2, GDPR, AI Actu nebo dalších standardů. Systém zároveň pomůže identifikovat chybějící pravidla, navrhnout potřebné směrnice, řídit nápravná opatření a průběžně sledovat riziko firmy v čase.

V Česku zatím neexistuje platforma, která by propojovala vzdělávání, testování a reporting do jednoho celku. V horizontu pěti let je naším velkým cílem expandovat dál na světové trhy. Aktuálně již aktivně řešíme vstup do Polska, Velké Británie i USA. Chceme se stát rovnocennou konkurencí pro největší globální hráče v kybernetické bezpečnosti. Důkazem, že jdeme správným směrem, je i fakt, že už dnes k nám od světových gigantů přecházejí korporátní klienti s tisíci uživateli.

Článek vznikl ve spolupráci s 4cyber.

**Expanze** *V Česku zatím neexistuje platforma, která by propojovala vzdělávání, testování a reporting do jednoho celku. V horizontu pěti let chce 4cyber expandovat dál na světové trhy.* **Foto: 4cyber**

▸Legislativa

**Adam Mašek**
adam.masek@hn.cz

# Digitální štít Evropy: Výrobci i prodejci se připravují na další dílek evropské obrany proti kyberútokům

Evropská unie spouští další vlnu významné kyberbezpečnostní regulace. Po směrnicích jako NIS 2, která se soustředí na bezpečnost kritické infrastruktury, a nařízení DORA pro finanční sektor přichází na řadu Cyber Resilience Act (CRA). Tentokrát se však pozornost bruselských zákonodárců neobrací k institucím, ale k samotným produktům. Cílem je vytvořit digitální štít, který ochrání firmy i spotřebitele před čím dál agresivnějšími kybernetickými útoky. Přísná pravidla budou zjednodušeně řečeno platit pro vše, co má v sobě kousek kódu a připojení k síti.

### Odpovědnost se vrací k výrobcům

Podstata CRA spočívá v zásadní změně paradigmatu: odpovědnost za kybernetickou bezpečnost se přesouvá z koncového uživatele na výrobce, dovozce a distributory. V praxi to znamená, že každý produkt s digitálním prvkem – od chytrých hodinek přes routery až po složité průmyslové řídicí systémy – bude muset splňovat striktní bezpečnostní standardy, aby mohl být uveden na trh EU.

„Cyber Resilience Act doplňuje evropskou směrnici NIS 2, která je v Česku implementována skrze Nový zákon o kybernetické bezpečnosti a cílí na bezpečnost infrastruktury a klíčových služeb. CRA má ale jiné zaměření: zatímco NIS 2 řeší bezpečnost organizací, CRA se soustředí na bezpečnost produktů," říká Jakub Höll, expert na kybernetickou bezpečnost a partner ve společnosti Deloitte. Produkty, které projdou přísným sítem, ponesou označení CE, které dnes známe například z elektroniky nebo hraček.

Regulace zavádí princip tzv. „security by design". Tedy požadavek, aby byla bezpečnost integrální součástí produktu již od jeho prvního návrhu, nikoliv jen dodatečně lepenou záplatou. Výrobci budou muset po celou dobu předpokládané životnosti produktu (minimálně pět let) bezplatně poskytovat bezpečnostní aktualizace a aktivně monitorovat veškeré zranitelnosti.

### Proč se o CRA mluví právě teď?

Ačkoliv nařízení formálně vstoupilo v platnost již v prosinci 2024, firmy nyní procházejí kritickým přechodným obdobím. Důvodem, proč se debata o CRA v posledních měsících zintenzivnila, je blížící se termín prvních ostrých povinností.

Podle Jakuba Neščivery, mluvčího Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), začne být regulace v praxi viditelná ve třech fázích. „V červnu 2026 nabývají účinnosti ustanovení týkající se oznamování subjektů posuzování shody. Následně v září nabude účinnosti ustanovení ohledně povinnosti hlásit aktivně zneužívané zranitelnosti a závažné incidenty," upřesňuje Neščivera s tím, že plná účinnost CRA nastane v prosinci příštího roku.

Zájem firem o téma roste úměrně s tím, jak si uvědomují komplexnost požadavků. „Přibližně od počátku roku se zájem společností o tuto problematiku začal zvyšovat. Subjekty se na nás obracejí zejména s dotazy ohledně výkladu jednotlivých pojmů a povinností," potvrzuje zvýšenou aktivitu byznysu Neščivera.

### Změna výrobních linek i dodavatelských řetězců

Dosah CRA je v Česku velmi široký. Na rozdíl od jiných předpisů se působnost neurčuje velikostí firmy, ale povahou produktu. Dopadne tak na malé softwarové domy i nadnárodní koncerny. Typickými zástupci jsou výrobci chytrých domácích spotřebičů, průmyslových senzorů, ale i mobilních aplikací a videoher. Výjimku mají pouze sektory s vlastní přísnou regulací, jako je automotive, zdravotnictví či letectví.

Pro řadu firem půjde o zásadní zásah do fungování. Budou muset vést tzv. SBOM (Software Bill of Materials). To je jakýsi detailní „seznam ingrediencí" veškerého použitého softwaru, podle kterého je možné identifikovat, kde se v případě útoku nachází slabé místo.

„Zásah do výroby a vývoje produktu může být pro řadu firem výrazný, zvlášť pokud dosud řešily kybernetickou bezpečnost spíše neformálně. Budou muset upravit procesy vývoje a testování a nastavit správu zranitelností," říká Kateřina Hůtová, manažerka kybernetické bezpečnosti a jednatelka společnosti Cybrela.

Specifickou výzvu CRA představuje pro velké prodejce a distributory, kteří se u vlastních značek stávají výrobci. Jakub Lasch, IT Director ve skupině HP Tronic vlastnící prodejce elektroniky Datart, k tomu uvádí: „Nařízení pro nás představuje výzvu ve dvou rovinách. Jako velký distributor budeme muset hlídat shodu u tisíců položek od různých dodavatelů. Druhou výzvou jsou naše privátní značky, například ETA. Zde budeme v roli výrobce a neseme odpovědnost za security by design a následné řízení zranitelností."

### NIS 2, DORA a riziko fragmentace

CRA nepřichází do prázdného prostoru. Je součástí komplexního legislativního balíku, který zahrnuje i směrnici CER (odolnost kritických subjektů), NIS 2 nebo sektorovou regulaci DORA pro finance. Právě tato provázanost je pro firmy dvojsečnou zbraní. Zatímco některé povinnosti se překrývají a usnadňují přípravu, jiné vytvářejí administrativní chaos.

Bankovní sektor se díky nařízení DORA cítí být na CRA připraven, přesto varuje před duplicitami. „Většinu povinností máme pokrytou v rámci DORA. CRA pro nás nepředstavuje drastické dopady, věříme, že povinnosti stihneme naplnit," říká Tereza Ryšanová, mluvčí Moneta Money Bank.

Kritičtější pohled na rostoucí počet regulací nabízí Jiří Raška, ředitel technologického rozvoje Partners Banky. „Problém není CRA, ale překryv pravidel. Jeden incident dnes musí banky hlásit do ČNB podle DORA, do NÚKIB podle NIS 2 a nově možná do ENISA (Evropská agentura pro bezpečnost sítí a informací – pozn. red.) podle CRA. Tři kanály, tři lhůty, jedna událost. Konsolidujte reporting do jednoho místa místo přidávání dalšího," vyzývá Raška.

### Investice versus administrativa

Otázka nákladů je pro firmy klíčová, avšak přesná čísla jsou v tuto chvíli stále v rovině odhadů. Experti se shodují, že u firem, které bezpečnost dosud podceňovaly, půjde o výrazné částky. V HP Tronic vnímají CRA jako masivní administrativní zátěž pro celý evropský řetězec, byť s pozitivní základní myšlenkou.

Banky mluví o stovkách milionů korun ročně investovaných do celkové bezpečnosti, do kterých se náklady na CRA „rozpustí". „Investice do ochrany klientů jsou součástí našeho rozpočtu, jakkoli nelze přesně vyčíslit náklady vyplývající pouze z implementace této regulace," konstatuje Filip Hrubý z České spořitelny. Podobně hovoří i Petr Milata za ČSOB, který nařízení považuje za přínosné pro klienty.

Zajímavý pohled nabízí softwarový průmysl. Marek Rosa, CEO Keen Software (výrobce herní série Space Engineers), upozorňuje na riziko „byrokratického divadla". „Kybernetickou bezpečnost bereme vážně už dnes – je to přirozená součást vývoje. Nechceme ale psát dokumenty jen proto, aby někde existovaly. Dodatečná práce bude pravděpodobně hlavně v přesnějším formálním popisu a dokumentaci," říká Rosa s tím, že pro tuto práci neplánuje najímat externí poradce.

### Hrozba likvidačních pokut a role státu

Motivace pro dodržování CRA je pro firmy nastavena prostřednictvím vysokých sankcí. Nejzávažnější porušení pravidel může vyústit v pokutu až 15 milionů eur (v přepočtu více než 360 milionů korun) nebo 2,5 procenta z celosvětového ročního obratu. Ještě větší hrozbou je však možnost zákazu prodeje produktu na celém trhu EU, což může být pro výrobce s jedním klíčovým produktem likvidační.

„Sankce jsou nastaveny extrémně vysoko. Z pohledu zákonodárce jde ale o logický nástroj k dosažení plošné compliance," podotýká Lasch. Podle Jiřího Rašky z Partners Banky je konkrétně pro finanční domy mnohem silnějším strašákem reputační riziko než samotná výše pokuty. Odpovědnost za kontrolu dodržování pravidel v Česku pravděpodobně připadne NÚKIB, i když legislativní proces ještě není u konce.

„Pracujeme se scénářem, kde bude NÚKIB zastávat roli oznamujícího orgánu, který jmenuje a dozoruje subjekty posuzování shody," uvádí Jakub Neščivera. Úřad se však nebude primárně věnovat dozoru nad trhem ve smyslu kontroly každého jednotlivého kusu zboží, ale spíše systémovému nastavení a metodické podpoře.

**Dosah CRA je v Česku velmi široký.** *Dopadne tak na malé softwarové domy i nadnárodní koncerny. Typickými zástupci jsou výrobci chytrých domácích spotřebičů, průmyslových senzorů, ale i mobilních aplikací a videoher.* **Foto: Shutterstock**

**~ Produkty, které projdou přísným sítem, ponesou označení CE, které dnes známe například z elektroniky nebo hraček.**

Inzerce

HN066353

# Lidé se nám nebojí zavolat, když mají problém s IT. A my jim pomůžeme

Když firemní e-maily začnou padat do spamu, většinou to nejdřív nevypadá jako velký problém. Obchodníci posílají nabídky, ale zákazníci neodpovídají. Faktury odcházejí, ale druhá strana je nevidí. Navenek všechno funguje. Jen se potichu ztrácí poptávky, čas a důvěra.

CX.TECH komplexní IT

Podobně začíná řada IT problémů ve firmách. Pomalé reakce dodavatele. Služby, které nějak běží, ale nikdo přesně neví jak. Nedostatek znalostí, když se objeví složitější problém. Pochybnost majitele, jestli je současné IT bezpečné a připravené na další růst.

**„Lidé se nám nebojí zavolat, když mají problém s IT. A my jim pomůžeme," říká Ondřej Hriadeľ, zakladatel brněnské IT firmy CX.TECH.**

Ondřej je technologický nadšenec, který chtěl od začátku dělat IT jinak. Ne jako anonymní linku, kde člověk zadá požadavek a čeká. Ale jako tým lidí, kteří mluví normálně, berou odpovědnost a umí firmě říct, co se děje. CX.TECH dnes pomáhá firmám po celé České republice, od Brna přes další kraje až po Prahu. Typicky jde o společnosti s 50 až 250 zaměstnanci, které už jsou dost velké na to, aby IT bylo kritické, ale ne vždy chtějí stavět vlastní IT oddělení.

Dřív často stačilo mít „někoho na počítače". Šikovného člověka, který opravil notebook, nastavil tiskárnu, zprovoznil e-mail a občas se podíval na server. Takoví lidé jsou pořád cenní. Jenže dnešní IT už je příliš široké na jednoho člověka.

Ve firmě dnes běží Microsoft 365, Google Workspace, účetní systémy jako Pohoda nebo Pamica, cloud, servery, Linux, sítě, zálohy, bezpečnost, vzdálená práce, přístupy zaměstnanců a stále častěji také požadavky kolem NIS2. Jeden člověk nemůže být současně síťař, M365 specialista, Google Workspace a Google Cloud specialista, člověk přes účetní software, serverový administrátor, Linux specialista a bezpečák.

**A přesně proto je tu CX.TECH a jeho tým specialistů.**

Proto dává smysl tým. Ne proto, že by jednotlivci byli špatní. Ale proto, že firma potřebuje jistotu, že se ke konkrétnímu problému dostane konkrétní odbornost.

V praxi to znamená, že když e-maily padají do spamu, neřeší se jen pošta, ale i domény, DNS záznamy, reputace a nastavení Microsoft 365 nebo Google Workspace. Když firma přesouvá e-maily z hostingu do Microsoft 365, nejde jen o technickou migraci, ale o to, aby lidé druhý den normálně pracovali. Když přijde ransomware nebo ztráta dat, rozhoduje připravenost záloh, sítě a krizového postupu.

Jindy je potřeba zauditovat celé IT, protože vedení firmy tuší, že „něco není dobře", ale neví přesně co. Nebo se segmentuje síť, aby se problém v jedné části firmy nerozlil všude. Konsolidují se servery, kde roky přibýval jeden systém přes druhý. Připravují se nové prodejny, aby od prvního dne fungovalo připojení, pokladny, zařízení, účty i podpora.

Vedle běžné správy roste i význam bezpečnosti. NIS2 pro část firem znamená konkrétní povinnosti, pro ostatní jasně ukazuje, kam se posouvá standard odpovědného řízení IT. CX.TECH nezačíná strašením ani paragrafy. Začíná otázkami, kterým rozumí každý majitel: kde máme důležitá data, kdo k nim má přístup, umíme je obnovit, co se stane při výpadku a kdo rozhoduje první hodinu po incidentu?

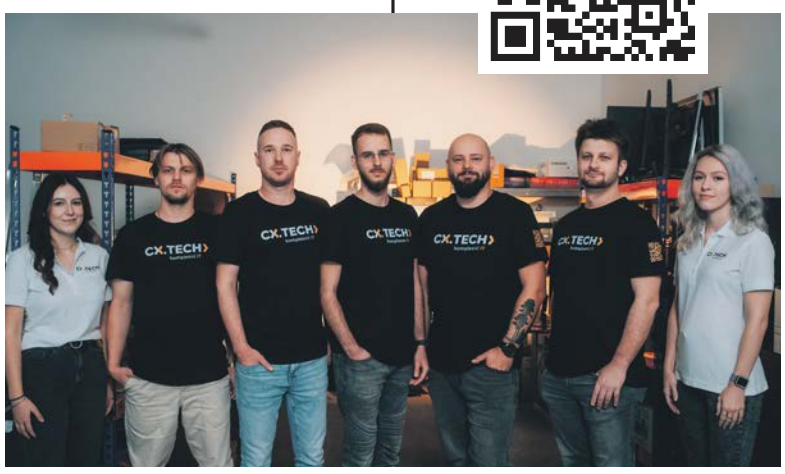
Na stejnou potřebu reaguje i CX_cloud, český cloud od CX.TECH. Je určený pro firmy, které chtějí mít důležité systémy a data v Česku, pod českým právem, s vysokou dostupností a zálohami navrženými tak, aby je útočník nemohl jednoduše smazat nebo zašifrovat. Nejde o to tlačit každého do cloudu. Jde o to najít řešení, které bude rychlé, bezpečné a nebude stát na jednom starém serveru v kanceláři.

To, co klienti na CX.TECH oceňují, není jen technická znalost. Je to i způsob komunikace. „CX Tech pro nás vyznačuje 100% spolehlivost, dostupnost a flexibilitu řešit IT problémy ihned. Vážíme si přímé, pohotové komunikace a zejména pozitivního přístupu k řešení jakéhokoliv IT problému," říká MUDr. Marcel Štelcl, Ph.D. z kliniky ReproGenesis.

**Cíl přitom není dělat z IT vědu. Cíl je, aby firma mohla fungovat. Aby e-maily docházely. Aby se data neztratila. Aby nové pobočky otevřely včas. Aby účetní systém neběžel na serveru, o kterém už nikdo moc neví. Aby podezřelý e-mail někdo zkontroloval dřív, než způsobí škodu.**

Pokud vaše IT stojí na jednom člověku, starém serveru nebo pocitu, že „nějak funguje", je dobrý čas si ho nechat zkontrolovat dřív, než vás k tomu donutí výpadek. CX.TECH vám pomůže zjistit, kde jsou největší rizika, co jde opravit hned a co má smysl řešit dlouhodobě. Stačí zavolat nebo napsat.

Kontakt email:
ondrej.hriadel@cxtech.cz




# Kybernetická bezpečnost začíná dřív, než dojde k útoku.

## Firmám pomáhají etičtí hackeři

**Kybernetické útoky dnes nepředstavují riziko jen pro velké korporace. Terčem hackerů se stále častěji stávají i menší a střední firmy, které často spoléhají na to, že nejsou pro útočníky dostatečně zajímavé. Realita je ale jiná. Únik dat, odstávka systémů nebo zneužití firemních účtů mohou znamenat finanční ztráty, poškození reputace i narušení důvěry zákazníků.**

Právě proto roste význam preventivních opatření. Jedním z nejúčinnějších způsobů, jak odhalit slabiny dříve, než je zneužijí skuteční útočníci, je penetrační testování. To nabízí společnost Haxoris, která se specializuje na oblast ofenzivní kybernetické bezpečnosti a etického hackingu.

**Když vás hacknou ti správní**

Penetrační testování je řízená simulace kybernetického útoku na firemní systémy, aplikace nebo webové stránky. Cílem není způsobit škodu, ale odhalit bezpečnostní nedostatky a zranitelnosti, které by mohly být zneužity při reálném útoku.

Etičtí hackeři z Haxoris přemýšlejí jako skuteční útočníci. Hledají cesty, jak se dostat k citlivým datům nebo získat neoprávněný přístup do systémů. Jakmile objeví slabé místo, klient získá detailní report s popisem rizik a konkrétními doporučeními, jak problém odstranit. Firmy tak dostávají jasný plán, jak zvýšit svou odolnost vůči kybernetickým hrozbám.

**Red teaming: simulace útoku bez kompromisů**

Ještě dál jde služba red teaming. Nejde jen o technické testování systémů, ale o komplexní simulaci reálného útoku, při které odborníci prověřují celkovou připravenost organizace.

Test může zahrnovat nejen online prostředí, ale i fyzickou bezpečnost firmy. Cílem je zjistit, zda by útočník dokázal jakýmkoli způsobem kompromitovat organizaci a získat neoprávněný přístup do jejích systémů, a to prostřednictvím technických zranitelností, lidských chyb nebo nedostatečně zabezpečených procesů. Součástí může být i získání citlivých informací, narušení interních systémů či převzetí kontroly nad vybranými prostředky organizace. Výsledkem je realistický obraz toho, jak by si firma vedla při skutečném útoku.

**„Nezadal jsem heslo, nic se nestalo." Největší mýtus o phishingu**

Ani sebelepší technologie nedokážou zcela eliminovat lidský faktor. Útočníci si to uvědomují a stále častěji využívají phishingové kampaně, jejichž cílem je přimět zaměstnance k prozrazení citlivých údajů nebo otevření škodlivého odkazu.

„Mnoho lidí žije v iluzi, že phishing je nebezpečný jen tehdy, když na podvodné stránce vyplní heslo nebo stáhnou podezřelý soubor. Realita je však tvrdší. Stačí jediný neopatrný klik a útočník může získat přístup do firemní sítě. Přestože je vícevrstvá bezpečnost nutností, technologie nezachytí 100 procent hrozeb. Poslední a zároveň nejdůležitější vrstvou ochrany je takzvaný lidský firewall," vysvětluje Andrej Šebeň, CEO společnosti Haxoris a etický hacker.

**„Mnoho lidí žije v iluzi, že phishing je nebezpečný jen tehdy, když na podvodné stránce vyplní heslo nebo stáhnou podezřelý soubor. Realita je však tvrdší. Stačí jediný neopatrný klik a útočník může získat přístup do firemní sítě. "**

Právě budování tohoto „lidského firewallu" je cílem platformy PhishGun. Nejde jen o službu, ale o self-service platformu pro realizaci phishingových kampaní, která firmám umožňuje bezpečně, kontinuálně a kontrolovaně testovat odolnost zaměstnanců vůči phishingovým útokům. Uživatelé si mohou jednoduše požádat o přístup do platformy, kde uvidí přehledné rozhraní a vytvoří svou první phishingovou kampaň zdarma. Simulované e-maily napodobují reálné scénáře, se kterými se zaměstnanci mohou setkat v praxi. Zaměstnavatel tak získá přehled o úrovni bezpečnostního povědomí týmů a zároveň identifikuje oblasti, na které je vhodné zaměřit další vzdělávání.

„Nezadal jsem heslo, nic se nestalo. To je jeden z nejrozšířenějších mýtů o phishingu. Kyberzločinci dnes využívají stále sofistikovanější techniky a často jim stačí jediná chyba uživatele. Proto je důležité nejen investovat do technologií, ale také pravidelně ověřovat připravenost zaměstnanců na skutečné hrozby," dodává Andrej Šebeň.

**Kybernetická bezpečnost jako součást firemní strategie**

Moderní kybernetická bezpečnost není pouze otázkou technologií. Jde o kombinaci kvalitního zabezpečení, správně nastavených procesů a informovaných zaměstnanců. Penetrační testování, red teaming i phishingové simulace pomáhají odhalit rizika ještě předtím, než se promění ve skutečný incident.

V době, kdy počet kybernetických útoků neustále roste, představuje proaktivní přístup jednu z nejlepších investic do stability a bezpečnosti každé organizace. Právě to je hlavním cílem etických hackerů – najít slabiny dříve, než je objeví někdo jiný.

HN066355

Inzerce

HN066311

Cybersecurity
Progress. Protected.

# AI PREVENCE PROTI HROZBÁM BUDOUCNOSTI

**Inteligentní prevence**
Ochrana před ransomwarem a phishingem na bázi AI

**ESET PROTECT**
Kyberbezpečnost celé firmy přehledně v cloudové platformě

**Služba MDR**
24/7 detekce a blesková reakce z rukou odborníků

www.eset.cz