PARADOXY KYBERSVĚTA

aneb

bezpečnost v nejistotě

MAREK KOVALČÍK

Upozornění pro čtenáře a uživatele této knihy

Tato kniha se věnuje principům, souvislostem a paradoxům kybernetické bezpečnosti. Jejím cílem je pomoci čtenáři lépe porozumět digitálnímu světu, jeho logice, slabinám i způsobům, jak o něm přemýšlet. Nejde o návod k obcházení pravidel, ale o snahu zasadit téma bezpečnosti do širších souvislostí.

I. vydání
ISBN 978-80-11-08858-3 (brožováno)
ISBN 978-80-11-08859-0 (pdf)
ISBN 978-80-11-08860-6 (ePub)
ISBN 978-80-11-08861-3 (Mobipocket)

Obsah

Věnováno všem, kteří si uvědomují, že technologie nejsou jen nástrojem pokroku, ale také zdrojem nových rizik.

V dnešní době už mnohdy přenecháváme většinu kreativních činností čistě systémům umělé inteligence. Tuto knihu jsem však napsal po staru – klávesnice, vlastní myšlenky i formulace. Ne proto, že bych nebyl fanda inovací a autonomních systémů. Nýbrž proto, že jsem to tak zkrátka chtěl. Je pravděpodobné, že by celou knihu zvládl správný AI model napsat během pár minut, a třeba i v lepší kvalitě. Místo této časové optimalizace jsem nad popisováním paradoxů strávil několik měsíců. Konzultoval s kolegy z praxe a texty nespočetněkrát upravoval. Mým cílem bylo přenést vlastní myšlenky na papír bez zkreslení či upřesňování natrénovaným modelem.

Úvodní slovo autora

Kyberbezpečnost není o hledání jedné správné odpovědi. Je o řízení rozporů bez jednoduchého řešení. A o neustálém rozhodování mezi nimi, kdy ani jedna volba není bez rizika.

Tato kniha volně navazuje na předchozí díl Nástrahy internetu, aneb informační (ne)bezpečnost, kde jsem vysvětloval principy hackerských útoků, zejména na bázi metod sociálního inženýrství. I zde zůstává hlavním tématem kybernetická bezpečnost. Tentokrát však nechci pouze popisovat hrozby ani hledat jednu správnou odpověď. Zaměřím se na rozpory, které se v bezpečnosti objevují stále znovu. Jeden pohled ukazuje hodnotu daného rozhodnutí. Druhý ukazuje cenu, kterou za něj platíme. Oba mohou být pravdivé zároveň.

Z fyziky víme, že každá akce vyvolává reakci. Dovolím si tento citát lehce rozšířit. Každá akce vyvolává

několik reakcí. Z pohledu informační bezpečnosti může být touto akcí změna v administrativních, operativních či technologických a dalších opatřeních. Přestože původním záměrem změny mohlo být zvýšit odolnost organizace či zefektivnit práci uživatelů, může tato akce vyvolat vlnu pozitivních i negativních reakcí. A přesně toto vnímám jako jednu z několika definic paradoxu.

Celá kniha bude věnována paradoxu a jeho podobám. Nejdříve si vysvětlíme blíže, co to paradox je a následně se vám pokusím předat konkrétní příklady rozdělené do pěti bloků, kdy každý z nich je trochu jinak tématicky zaměřený. Principy jednotlivých paradoxů budu popisovat od nejširší perspektivy k té nejkonkrétnější. Od strategického rámce, přes technologickou realitu k lidskému faktoru. Následně přejdeme k řízení, odpovědnosti a rozhodování. A nakonec k budoucnosti.

Předchozí kniha Nástrahy internetu byla cílena na širokou veřejnost se snahou šířit všeobecné povědomí o kybernetických hrozbách a jak se před nimi chránit. Paradoxy kybersvěta na problematiku pohlíží více abstraktně a cílí na manažery kybernetické a informační bezpečnosti, IT ředitele a specialisty, majitele firem a zástupce leadershipu v organizacích. Kniha pojednává

o strategických tématech, jejichž začlenění do konkrétních procesů a technologií jednotlivých organizací se může velmi lišit.

Účelem knihy je, aby čtenář pochopil, proč je téma strategické kybernetické bezpečnosti důležité. Následně zjistí, co bývá příčinou problémů, jakou roli v něm hrají lidé a kdo nese odpovědnost. A nakonec, jaké výzvy a rizika přináší budoucnost.

Tak pojďme na to!

Co je to paradox?

Než se hlouběji ponoříme do jednotlivých kapitol, je nutné si vymezit základní pilíř celé knihy – paradox. Paradox není chyba systému ani slovní hříčka. Je to napětí mezi dvěma pravdami, které vedle sebe současně platí, i když se na první pohled vylučují. Paradox by neměl čtenáře rychle uklidnit. Má ho na chvíli zastavit a donutit připustit, že bezpečnost není soubor správných odpovědí, ale práce s nejistotou, která nikdy úplně nezmizí.

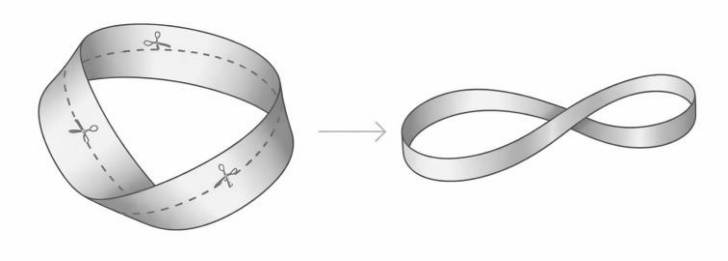
V kybernetické bezpečnosti se často neptáme, která volba je správná. Ptáme se, jak řídit rozpor, ve kterém žádná volba není bez rizika. Uvědomění si tohoto napětí je začátek hlubšího pochopení dané problematiky.

How wonderful that we have met with a paradox.
Now we have some hope of making progress.

\- Niels Bohr

Stejně jako v předchozí knize nebudu sáhodlouze citovat a opakovat přesné definice, naopak se vždy snažím komplexní témata prezentovat jednoduše. Proto bych chtěl demonstrovat pojetí paradoxu na jednoduchém experimentu. Ten se nazývá Möbiova páska, což je paradoxní objekt objevený A. F. Möbiem a J. B. Listingem v roce 1858. Ač to na první pohled může znít složitě, experiment je velmi jednoduchý a věřím, že mnoho z nás se s ním setkalo už na základní škole.

K vytvoření tohoto paradoxního objektu nám stačí tenký proužek papíru, jehož konce slepíme tak, aby levý roh první strany byl připevněn na pravý roh druhé strany. Vznikne útvar zobrazený na obrázku 1 v levé části.



Obr. 1 - Möbiova páska

Tento paradoxní útvar má několik zajímavých vlastností. První z nich je, že má pouze jednu stranu. Pokud budete kreslit čáru po jeho obvodu, nakonec dojdete na místo, odkud jste kreslit začali. Stejně tak má objekt pouze jednu hranu. Pokud pojedete prstem po hraně papíru, vždy se nakonec vrátíte do stejného výchozího místa. Paradoxní objekt má tedy jen jednu stranu a jednu hranu, přesto je stále trojrozměrný.

Ještě zajímavější pokus je rozstřihnutí pásky. Pokud ji budete stříhat ve středu šířky papírku, po úplném rozstřižení objekt stále zůstává pohromadě, jen se zdvojnásobuje jeho obvod. Pokud budete stříhat blíže ke kraji po celé délce, vytvoří se nová vnořená Möbiova páska.

Ano, jedná se o jednoduchý dětský experiment. Ukazuje nám však, že realita může být zkreslena naším intuitivním vnímáním. Ukazuje nám, že akce vyvolaná na objektu může vést k jiným výsledkům, než jsou na první pohled očekávané.

V kontextu kybernetické bezpečnosti – můžeme chránit pouze to, co známe a víme, že máme. Musíme domýšlet všechna možná rizika plynoucí z implementací změn. Přitom nelze vždy vycházet pouze ze zkušeností. Musíme uvažovat i nad riziky, která nejsou na první

pohled zřejmá a mohou mít příčinu v malých detailech implementovaných změn. Bezpečnost je kontinuální proces, nikoli jeden časový bod, od kterého bychom si mohli říci, že jsme naprosto bezpeční. Je to kombinace hardwarových i softwarových řešení, procesů, směrnic, příruček a manuálů, školení, kultury i osvěty. A to vše je třeba neustále rozvíjet, aktualizovat, zlepšovat. Musíme zohledňovat změny, které kybernetický svět přináší nepřetržitě. Paradoxy můžeme najít ve všech zmíněných částech, což se Vám budu snažit dokázat v této knize.

Možná právě v tom je první paradox této knihy: čím více chceme bezpečnost vysvětlit, tím snadněji můžeme ztratit napětí, které nás o ní nutí přemýšlet.

I. Strategie

Strategie v bezpečnosti není mapa bez rizika. Je to volba rizika, které jsme ochotni nést, a rizika, které už nést nesmíme. Kybernetická bezpečnost je proces. Musí být neustále monitorována, řízena a zlepšována. A to především na úrovni vedení organizace. Nejedná se o technický doplněk, ale o klíčovou součást firemní strategie, která má přímý dopad na podstatu moderního byznysu.

V menších podnicích je stále často až na druhé koleji a z určitého pohledu je to naprosto pochopitelné. Pro začínající firmy je mnohem důležitější rychle proniknout na trh a generovat zisk. Proto je mnohdy IT řízeno punkově, změny jsou realizovány bez hlubšího promýšlení či testování. Náprava chyb a řešení incidentů není tak drahé, jako pro vyzrálou firmu.

Větší podniky si uvědomují, že odstávka systému z důvodu řešení bezpečnostního incidentu je mnohem dražší, než investice do prevence. Mimo přímé náklady související s obnovou, nákupem hardware, licencí,

náklady na zaměstnance, kteří nemohou pracovat, přichází také velké náklady spojené s ušlým ziskem. Například, když stojí linky výrobního podniku, který jinak funguje v nepřetržitém provozu. Proto větší společnosti musí bezpečnost zakomponovat do své strategie. Nejedná se však jen o výrobní podniky. Nemožnost používat IT infrastrukturu z důvodu kybernetického útoku se může vléct dny i týdny, což je významná hrozba i pro nevýrobní podniky.

Riziko tedy nevzniká až v momentě, kdy je IT infrastruktura a systémy společnosti funkční a stabilní. Vzniká už ve chvíli, kdy se firma rozhodne růst, digitalizovat, inovovat a být efektivnější. Zranitelnostem odhaleným již během návrhů strategie je mnohem snazší a levnější předcházet. Dalo by se říct, že zde vzniká tenká hranice mezi ambicí a zranitelností.

Paradox digitalizace

V dnešním světě, ve kterém jsme zvyklí využívat moderní technologie každý den, si už jen těžko dokážeme představit návrat ke starším způsobům zpracovávání a uchovávání informací. Odeslat e-mail je mnohem rychlejší a pohodlnější než odeslat papírový dopis. Archivovat dokumenty na cloudovém úložišti je mnohem efektivnější, než uchovávat papírové svazky v nekonečném množství šanonů. Je to digitalizace, která nám pomáhá optimalizovat procesy, urychlovat získávání, vyhodnocování a zpracování dat a informací. Čím více převádíme svět do digitální podoby, tím více jej dokážeme řídit. A tím více stačí jediná skrytá chyba, aby se řízený svět změnil v závislý.

Spoustu hrozeb spjatých s nedigitálními přístupy odstraňuje. Přesto je to paradoxně digitalizace, která vytváří zranitelnosti, které před ní neexistovaly. Žádná technologie není dokonalá a systémy mohou obsahovat bezpečnostní díry, které bývají následně zneužity útočníky k infiltraci aplikací, systémů či jejich částí. Dokazuje nám to také fakt, že i ti největší technologičtí giganti se neustále potýkají s kybernetickými incidenty,

vydávají aktualizace s bezpečnostními záplatami a věnují se inovacím stejně usilovně jako bezpečnosti.

Digitalizace procesů je rozhodně krok správným směrem. Je však nutné myslet i na to, že čím více firma digitalizuje, tím roste i prostor pro chyby a zneužívání zranitelností. Digitalizace přináší rychlost, škálování a nové obchodní modely. Současně ale rozšiřuje útočný potenciál, zvyšuje závislost na technologiích a vytváří nové cesty k selhání.

Paradox růstu

Každý z nás se může stát obětí kybernetického útoku. Troufám si říci, že každý čtenář této knihy se už někdy setkal s podvodným e-mailem - phishingem. A to v osobním i pracovním prostředí. Vytvořit a hromadně rozeslat velké množství podvrhů z mnoha různých adres je pro hackery relativně jednoduchá a levná záležitost. Setkáváme se s phishingy často právě z důvodu jejich poměru složitosti zpracování a dopadu úspěšně napadeného počítače či ukradené identity uživatele.

Zjednodušeně řečeno – útočník může rozeslat automatizovaně stovky podvodných zpráv a pokud se mu povede ulovit alespoň jednoho uživatele, může to být jeho vstupenka k infiltraci dalších částí sítě.

Složitější a dražší jsou z pohledu útočníka takové útoky, které vyžadují hlubokou přípravu, detailní analýzu cíle a využití technik infiltrace, které nebudou okamžitě odhaleny. Cílem bývají často významné osobnosti nebo organizace. Čím úspěšnější organizace je, tím zajímavější je i pro útočníky. Taková organizace běžně pracuje s citlivými daty, má množství klientů i zaměstnanců, více finančních prostředků a řešení kybernetického incidentu nebo odstávka systémů ji bude stát nemalé peníze, oslabení nebo dokonce ztrátu reputace.

Růst znamená více zákazníků, dat, systémů i peněz. To vše zvyšuje atraktivitu firmy jako cíle a mění bezpečnost z podpůrného tématu na strategický.

Paradox inovace

Dalo by se říci, že inovace jsou hnacím motorem, který vytváří konkurenční výhody. Pokud společnost nebude dostatečně inovovat, může se dostat naopak do fáze stagnace. To se dá volně počeštit jako období bez růstu, ustrnutí či uváznutí. Minulost nám již několikrát ukázala, že firmy, které začaly stagnovat, následně začaly ztrácet tempo vůči konkurenci a jejich hospodářská činnost klesala. V některých případech společnosti úplně zanikly. Inovace tedy nejsou pouze to, co firmu posouvá vpřed, ale také ji drží naživu.

Smyslem inovací bývá zvýšení efektivity nějakého procesu či vytváření nových hodnot a výhod. Jenže právě tady paradox začne být nepohodlný. Každá inovace řeší problém. A vytváří další. Ne proto, že by inovace sama o sobě byla špatně, ale protože do prostředí přináší nový prvek, novou závislost, nová data a nový způsob použití. Názorným příkladem je masivní vzestup systémů umělé inteligence. Dnes už jsme ve stavu, kdy umělou inteligenci využíváme na denní bázi. Řeší za nás rutinní úkoly, pomáhá zpracovávat velká data a navrhovat řešení. Lidé byli a jsou možnostmi inteligentních

systémů natolik ohromeni, že bezpečnost zpracovávaných dat se začala na firemní úrovni řešit až mnohem později. Například, jaká data jsou využívána? Jak jsou zpracovávána? Kde jsou ukládána, jak jsou přenášena a kdo všechno k nim má přístup?

Nové služby, produkty a digitální kanály posouvají firmu vpřed, ale téměř vždy otevírají nové bezpečnostní otázky, na které organizace nebývá připravena. Čím více inovujeme, tím více rozšiřujeme prostor, který neumíme bezpečně uchopit. Inovace vytváří hodnotu. A současně vytváří nové slabiny. Inovace nejsou problém. Problém je víra, že jejich dopad máme vždy plně pod kontrolou.

Paradox rychlosti

Často můžeme slýchávat, že tato doba je „velmi rychlá“ – co to ale znamená? Co si pod touto frází představit s ohledem na kybernetickou bezpečnost?

Digitální revoluce se obvykle datuje od poloviny 20. století, kdy vynález tranzistoru umožnil vznik moderních počítačů a postupnou digitalizaci informací. Významný moment přišel s formulací Moorova zákona v roce 1965. Ten říká, že počet tranzistorů na čipu (a tedy i výpočetní výkon) se zhruba každé dva roky zdvojnásobuje. Tento exponenciální růst způsobil, že technologie se nezačaly vyvíjet lineárně, ale stále rychleji – od prvních sálových počítačů přes osobní počítače až po dnešní propojený svět internetu a umělé inteligence.

Tento trend rychlosti růstu se netýká pouze technologií, ale také firem. Ty jsou mnohdy na technologiích přímo závislé, což je nutí držet krok a rychle inovovat. Čím rychleji organizace mění systémy, tím obtížnější je chránit.

Čím rychlejší jsme, tím méně máme pod kontrolou to, co jsme vytvořili. Rychlost vyhrává trh. Bezpečnost rozhoduje, jestli na něm přežijeme. To, co

dnes nasadíme, už zítra nemusíme umět ochránit. A přesto to často nasadit musíme.

Byznys chce jít rychle. Bezpečnost chce zpomalit. Obě strany mají pravdu. A právě proto nelze mít obojí naplno. Rychlost sama o sobě není problém. Problém je víra, že ji dokážeme řídit bez toho, aby něco unikalo. Brzdy nejsou proto, aby firma zastavila. Jsou proto, aby mohla jet rychle.

Paradox efektivity

V předchozí kapitole jsme si povídali o digitalizaci a růstu, rychlosti a inovacích. Dalším přímo návazným faktorem je zvýšení efektivity práce. Neustálý tlak na zvyšování efektivity procesů, lidí a technologií je všudypřítomný. Má to své opodstatnění. Čím je firma ve svém počínání efektivnější, tím více zisku je schopna generovat.

I zde však můžeme najít paradox. Zvyšování efektivity je často spjato s automatizací činností. Čím

efektivněji firma funguje, tím méně prostoru má pro chybu. Čím menší prostor pro chybu, tím lépe. Nesmíme však ztratit schopnost chyby vyhledávat a napravovat i v automatizovaných efektivních procesech. Čím méně rezerv v systému ponecháme, tím lépe funguje za normálního stavu. A tím hůř snáší stav, pro který jsme rezervy odstranili.

Optimalizace procesů často odstraňuje rezervy, redundanci a manuální kontroly. Bezpečnost pak mnohdy doplácí na to, že prostředí je sice rychlé, ale křehké.

Paradox centralizace

Znám techniky i šéfy firem, kteří jsou zapřisáhlí podporovatelé centralizovaného přístupu k řízení IT. Pojem decentralizované řízení je pro ně noční můrou. Je však centralizované řízení opravdu ten jediný správný přístup?

Centralizovaná správa umožňuje jednomu člověku či skupině lidí řídit provoz, politiky, přístupy, infrastrukturu, identity. Umožňuje efektivnější kontrolu a rychlejší reakci na incidenty. Sloučení identit, nástrojů a infrastruktury může přinést větší přehled a snížit náklady. Jeden řídicí bod přináší přehled. A zároveň vytváří místo, jehož selhání bolí nejvíc.

Centralizace zvyšuje kontrolu, ale také zvětšuje dopad případného selhání. Když selže centrální bod, následky bývají systémové a kritické. Není to však jen o selhání. Centralizované systémy vytvářejí obecně menší flexibilitu pro týmy a omezují možnosti inovací a růstu.

Paradox decentralizace

Jako další se přímo nabízí zaměřit se na decentralizované řízení. To má také své plusy i mínusy a několik paradoxů.

Decentralizace je často spjatá s větší autonomií týmů. Jednotlivé týmy, pobočky či jiné organizační jednotky mají více možností vlastního rozhodování. Ať už se jedná o nákup konkrétních technologií, nastavení pravidel, bezpečnosti či kultury. Decentralizovaný přístup je často spjatý s rychlejším růstem a inovacemi. Také není závislý na jednom konkrétním dodavateli.

Vhodně nastavená decentralizace stejně jako její opak, centralizace, zvyšuje odolnost firmy. Většinou ale za cenu, že snižuje celkový přehled. Zvyšuje také riziko Shadow IT a Shadow AI, což je neoficiální používání hardwaru a softwaru mimo kontrolu IT administrátorů.

Distribuované prostředí omezuje existenci jednoho kritického bodu. Na druhou stranu komplikuje dohled, správu a jednotné řízení bezpečnosti, což se může promítnout také do obtížnější reakce na případné incidenty.

Paradox kontroly

Všichni chceme mít kontrolu nad svými systémy a daty. Nezáleží na tom, jestli jsme fyzická či právnická osoba. Bez kontroly nastává chaos, a ten je nechtěný. Existuje však něco jako absolutní kontrola?

Můžeme se snažit mít kontrolu nad svými procesy, systémy i daty. Nikdy však nebude absolutní, a to z prostého důvodu – černé skříňky. Jedná se o princip používání systému, jehož přesné interní fungování nám zůstává skryto. Když bychom se zamýšleli nad tímto paradoxem více, pro absolutní kontrolu bychom museli znát fungování každého kusu hardware i software do posledního detailu. To je nejen neefektivní, ale často také nemožné.

Troufám si tvrdit, že černé skříňky využíváme všichni denně. Od telefonů, přes počítače, informační systémy a komunikační platformy. Můžeme aplikovat různá bezpečnostní opatření a minimalizovat širokou škálu rizik. Přesto bude naše kontrola vždy jen omezená. Kontrolu posilujeme tím, že přidáváme další vrstvy řízení. A každá nová vrstva nám současně něco skrývá.

Paradoxem také je, že obecný trend směřuje k tomu se kontroly dobrovolně vzdát. S ohledem na informační technologie narážím na migrace infrastruktury a aplikací do různých cloudových řešení. Jejich využívání nám pomáhá zefektivňovat fungování a snižovat určitá informační rizika. Částečně se však vzdáváme té části kontroly, kterou ještě máme.

Organizace chtějí mít IT pod kontrolou – ale jejich infrastruktura je stále více mimo jejich kontrolu. Cloud, software jako služba a externí dodavatelé znamenají, že kritické systémy jsou často mimo přímou správu firmy.

Paradox akvizic

Běžnému člověku jsou akvizice často skryté, ale v byznys prostředí se jedná o běžnou součást životního cyklu firem. Jedná se o praktické převzetí jedné společnosti druhou. Cílem je obvykle růst, získat větší tržní podíl nebo nové zdroje.

Akvizice zvyšují hodnotu firmy, ale přinášejí cizí rizika. Existuje několik dobře zdokumentovaných případů kybernetických útoků, kdy se kompromitace menší nebo cílové společnosti během akvizice stala vstupní branou k úspěšnému útoku na větší organizaci.

Souvisí to například s nevyzrálostí bezpečnostní strategie kupované společnosti či neefektivitou jejího bezpečnostního programu. Reálné kybernetické útoky mohou trvat i měsíce. Aby byly úspěšné, musí útočník nejdříve infiltrovat kritické systémy. Je to typické zejména pro ransomwarové útoky. V případě, že dojde k synchronizaci či integraci napadených aktiv společnosti, může se útok promítnout také do infrastruktury nakupující firmy.

Při fúzích a akvizicích (M&A) firma často získává i cizí technický dluh. Pod tímto termínem si můžeme představy zastaralé IT systémy, neznámé identity, chybné konfigurace či neodhalené kompromitace. Jedná se pak o selhání kybernetické due diligence v procesu akvizice. Akvizice kupuje hodnotu, kterou vidíme. A současně přebírá riziko, které často vidět není.

Paradox závislosti

Firmy digitalizují, inovují a zefektivňují svou činnost. Přechod zpět od informačních systémů k papírům a šanonům je už naprosto nemyslitelný. Žijeme v době, kdy jsme naprosto závislí na funkčnosti IT systémů. Jejich neustálou dostupnost, spolehlivost a bezpečnost bereme jako samozřejmost. Mnohdy si uvědomíme křehkost celého ekosystému až v momentě, kdy nastane nějaký incident. Může se jednat o kybernetický útok, výpadek napájení, logickou chybu v systémů či nedostupnost klíčového dodavatele. Všechny tyto a mnohé další incidenty mají za následek to, že zaměstnanci nemohou pracovat, firma nemá přístup ke klíčovým systémům či datům, což se přímo promítá do finančních či reputačních ztrát.

Incidentům nelze se stoprocentní účinností zabránit. Budou nastávat vždy. Můžeme na ně však být vhodně připraveni. Narážím na plány obnovy, plány reakce na incidenty a katastrofy, řízení rizik a plány zálohování. Čím více je firma technologicky vyspělá, tím méně umí fungovat bez technologií. Čím více je firma

technologicky vyspělá, tím náročnější je tyto procesy implementovat a spravovat.

Moderní organizace jsou stále efektivnější, ale zároveň ztrácejí schopnost nouzového provozu bez klíčových systémů. Technologie nám dávají svobodu dělat víc. A právě proto se bez nich přestáváme umět obejít.

II. Technologie

Technologie, zejména informační technologie, se zdokonalují obrovskou rychlostí. Téměř každý den se na trh dostávají nové aplikace, nové systémy, noví dodavatelé. Nepopírám, že významné pokroky se dějí neustále i v jiných oborech. Jako technik zaměřený na informační a kybernetickou bezpečnost se však budu i v této kapitole držet tématu paradoxů kybersvěta.

Firmy se chtějí aktivně chránit. To znamená držet krok s inovacemi v oblasti technologií. Existuje spousta bezpečnostních prvků zaměřených na jeden konkrétní problém. Také technologie kombinující více prvků do jednoho systému, který má za úkol řešit více problémů najednou. Integrováním více systémů dohromady vzniká relativně křehký ekosystém, kde narušení jedné významné části může mít přímý dopad na fungování všech ostatních. A tedy i chodu celé společnosti. Moderní technologie nás současně chrání i komplikují naši obranu.

Tato část rozebírá, proč se technické prostředí stává těžko uchopitelným, proč samotné nástroje nestačí a proč se z obrany často stává další vrstva rizika. Je to blok o komplexitě, propojenosti a vedlejších účincích technologického pokroku.

Paradox komplexity

Občas slýchávám, že se v dnešní době řeší jednoduché problémy složitě, což zvyšuje časovou i finanční náročnost provedení. Je tomu opravdu tak? Opravdu se inženýři snaží jenom nafukovat jednoduché problémy, aby mohli fakturovat více? Opravdu je nutné mít nyní k dispozici tým několika úzce zaměřených specialistů, když to dříve nebylo potřeba?

Složitost nevzniká proto, že by ji někdo chtěl. Vzniká proto, že chceme jednoduchost pro uživatele. Neustále roste obecný tlak na to, aby síťová spojení byla rychlejší. Aby připojení bylo stabilnější. Aby aplikace byly intuitivnější a zároveň přibývaly nové funkcionality.

Roste tlak na to, aby systémy byly odolnější, zejména při velkém objemu zpracovávaných dat a zapojených uživatelů. Chceme přistupovat k aplikacím odkudkoliv a kdykoliv. V neposlední řadě chceme mít garantovanou bezpečnost.

Nemyslím si, že moderní doba je o umělém vytváření a následném řešení problémů, které dříve neexistovaly. Naopak je rostoucí komplexita celého IT důsledkem neustále rostoucí poptávky uživatelů a organizací.

Konkrétním příkladem může být hojně využívaný internetový obchod v období vánočních svátků. Takový obchod musí počítat s nárůstem počtu uživatelů a rychle se měnícím sortimentem zboží. Po skončení onoho hektického období nejspíše poptávka opět na čas ustane. Jak se na takový problém připravit s ohledem na minimalizaci nákladů? Podobné obchody často fungují v nějakém cloudovém prostředí, které umožňuje jednoduše škálovat výpočetní zdroje. To znamená, že klient platí pouze za výpočetní výkon, který reálně používá a může jeho množství v čase dynamicky měnit. Zároveň není problém přidávat technologie pro řízení zátěže. V případě enormního příchodu uživatelů na e-shop se technicky směruje provoz na několik serverů,

které operují samostatně a jsou řízeny centrálně, aby nedošlo k jejich přetížení. Říká se tomu load balancing.

Do větších technických detailů tento příklad rozebírat nechci. Myslím, že dobře demonstruje nový přístup k řešení starých problémů. Dalo by se říct, že v dřívějších dobách, kdy primárním zdrojem zboží byly pro uživatele pouze kamenné prodejny, by stejný způsob řešení vyžadoval více obchodních domů či poboček. Ty by navíc bylo nutné dynamicky otevírat a zavírat dle aktuálního množství příchozích zákazníků.

Z pohledu uživatele nám nezáleží na tom, jak je konkrétní problém řešen. Pouze chceme, aby vyřešen byl. A to bez narušení našeho komfortu. Z pohledu administrátorů informačních technologií tohoto cíle dosahujeme kombinováním více nezávislých prvků a jejich efektivní správou, udržováním a dalším rozvojem. Čím sofistikovanější infrastruktura je, tím méně jí lidé skutečně rozumějí. Moderní prostředí je složené z tolika vrstev, integrací a závislostí, že úplné porozumění je pro jednoho člověka prakticky nemožné.

Paradox spolehlivosti

Zajištění spolehlivosti používaných systémů a aplikací je jedním z důležitých cílů jejich administrátorů. Ve škole jsme spolehlivost počítali na základě matematické pravděpodobnosti a statistiky. To však není ten přístup, který vám zde chci přiblížit. Místo toho bych chtěl poukázat na několik manažerských pohledů, které mohou odhalit nespolehlivost v jinak spolehlivě vypadajícím systému.

Systém plní požadovanou funkci a nehlásí žádné chyby. Je tedy spolehlivý? Může být i nemusí. Žádná technologie není dokonalá a dlouhodobá absence chyb může spíše poukazovat na neošetřené vstupy, nedokonalé integrace či neimplementované funkcionality. Tyto potenciální nedostatky mohou přímo ovlivňovat logický proces i data, a to bez upozornění na chybový stav. Čím zdánlivě spolehlivěji technologie fungují, tím více jim lidé slepě důvěřují. Dlouhodobě stabilní bezproblémový provoz snižuje ostražitost a posiluje přesvědčení, že systém je bezpečný.

Systém často hlásí chyby. Při chybě se jeho činnost zastaví a není možné jej používat. Je tedy

nespolehlivý? Může být i nemusí. Chyby mohou signalizovat procesní, funkcionální nebo technologické nedostatky. Stejně tak však mohou signalizovat neočekávané uživatelské vstupy či kybernetický útok. Množství kontrolních mechanismů může způsobovat nedostupnost, nicméně v případě chyby může být tato technologie skutečnou záchrannou brzdou. Zejména pro organizace, kde integrita a důvěrnost informací je mnohem důležitější, než jejich dostupnost. Řídíme se zde heslem – „raději ať nefunguje, než ať funguje blbě“. V takovém případě by se určitě jednalo o spolehlivý systém, nehledě na množství hlášených chyb.

Systém může fungovat správně právě proto, že se včas zastaví. A může vypadat spolehlivě právě tehdy, když potichu chybuje.

Paradox bezpečnostních nástrojů

Není možné veškerou počítačovou komunikaci neustále manuálně monitorovat a vyhodnocovat. Z pohledu zajištění potřebných finančních a lidských kapacit takový přístup nedává žádný smysl. Přesto je člověk velmi důležitou součástí bezpečnostního řetězce. Pokud má takový člověk, ideálně tým, k dispozici vhodné bezpečnostní nástroje, odolnost organizace rapidně roste. Potřebujeme využívat bezpečnostní nástroje, které z velké části fungují autonomně. Mohou to být například firewally oddělující a ochraňující perimetry sítí. Mohou to být skenery zranitelností, které periodicky porovnávají dostupné služby s databázemi známých zranitelností a upozorňují nás na případná nová odhalení. Mohou to být systémy monitorující síťový provoz s cílem odhalovat anomálie. Jsou to pokročilé systémy, které korelují informace z různých zdrojů pro skládání informací dohromady. Jsou to autentizační a autorizační systémy, je to šifrování, systémy zabezpečení koncových zařízení, zálohování a spousta dalších.

Bezpečnostních nástrojů pro podporu detekčních i reakčních procesů je nespočet a jejich popis včetně efektivního využití by byl na samostatnou knihu. Cílem této kapitoly je stručně ukázat, že žádná jediná černá kouzelná skříňka bezpečnost firmy opravdu nezaručí a že musíme integrovat více technologií dohromady.

Nástroje nás chrání před chaosem. Příliš mnoho nástrojů ale může vytvořit chaos vlastní. Více bezpečnostních technologií neznamená automaticky více bezpečnosti. Nástroje bez vhodné bezpečné integrace, ownershipu a definovaných procesů často vytvářejí jen iluzi ochrany a další provozní složitost. Také je velmi důležité mít dostatek provozních kapacit nejen k pořízení bezpečnostních technologií, ale i k jejich obsluze a neustálému zlepšování. Nezačíná tedy skutečná bezpečnost až tam, kde končí pouhé hromadění nástrojů?

Paradox viditelnosti

V předchozí kapitole popisující paradox bezpečnostních nástrojů jsem nastínil používání systému pro monitoring. Monitoring je velmi důležitý, protože pokud nejsme schopni hrozbu detekovat, těžko na ni budeme reagovat. Když nevidíme nic, jsme slepí. Když vidíme všechno, můžeme oslepnout šumem.

Do kategorie detekčních bezpečnostních opatření můžeme zahrnout například firewally, antivirová a behaviorální opatření na koncových stanicích (antiviry a EDR), síťové sondy, systémy prevence úniku dat (DLP) a další. Některé z těchto systémů mohou nad rámec detekce zároveň plnit funkce preventivních či nápravných opatření.

Ve větších organizacích bývají často všechna tato řešení implementována. Monitorujeme tedy zařízení, sítě, uživatele, hranice společnosti. Monitorujeme je v digitálním i fyzickém světě. V takový moment už se dá říci, že viditelnost sítě je zajištěna relativně dostatečně. Nastává však nový problém. Čím více monitorujeme, tím snazší je přehlédnout to podstatné.

Má-li společnost již takto silnou základnu bezpečnostních technologií, dává smysl přemýšlet nad tím, jak sbírané informace vhodně vyhodnocovat. Jak z nich získávat užitečné znalosti? Jak detekovat pokročilé hrozby, motivované útočníky a vhodně na jejich aktivity reagovat? Jak efektivně zpracovávat takovou záplavu informací? Využívají se k tomu například nástroje SIEM (Security Information and Event Management). Ty dokážou zpracovávat velké množství dat, vyhodnocovat souvislosti a notifikovat administrátory s doporučeními pro mitigační zásahy.

Také na tyto centrální vyhodnocovací systémy mohou být napojeny automatizované akce, ale mnohdy jsou stále obsluhovány specialisty v oboru. Paradoxně problémem již není nedostatek dat. Jejich množství je novou výzvou pro zlepšování schopnosti oddělit signál od šumu. Dalším paradoxem je, že při snaze automatizovat a zlevnit detekční a reakční schopnosti dochází k významným investicím do technologií, které musí spravovat odborně proškolení a často drazí specialisté.

Paradox dat

S množstvím implementovaných procesů a technologií narůstá také množství dat, které organizace musí vhodným způsobem systematicky shromažďovat, vyhodnocovat a uchovávat. S tím nám pomáhají technologie, avšak ani nejmodernější systémy nejsou dokonalé a v detekci mohou vznikat chyby a šum. Data mají zmenšovat nejistotu. Při špatném kontextu ji však pouze přesněji pojmenují.

Jedním z příkladů takových chyb mohou být falešně pozitivní nálezy. Jedná se o detekce, nebo například incidenty, které vyžadují zásah bezpečáků. V průběhu jejich vyhodnocení se však dojde k závěru, že upozornění není relevantní. Může jít o konfigurační či logickou chybu v pravidlech na detekčním systému, který upozornění zasílá. Přestože se u falešně pozitivních nálezů nejedná o narušení bezpečnosti, nejsou tyto stavy chtěné, jelikož zdražují provoz. Zdražují ho právě plýtváním času bezpečnostního týmu na ladění reálně neexistujících chyb.

Druhým příkladem je falešně negativní nález. Ten je s ohledem na první příklad mnohem vážnější.

Falešně negativní nález se prokáže až s odstupem času, kdy byl útočníkův pokus špatně vyhodnocen jako legitimní akce a nebyl blokován. Útočník se tak vyhnul detekci i reakci bezpečnostního týmu. Falešně negativní nálezy jsou mnohem náročnější na odhalení, protože na ně bezpečnostní technologie principiálně neupozorňují.

Čím více dat organizace sbírá, tím obtížnější je rozpoznat skutečný útok. Bez monitoringu a sběru dat však narušení bezpečnosti zjistit nelze. Bez dostatečného kontextu a prioritizace se z dat stává hluk, který zpomaluje reakci a snižuje jistotu rozhodování.

Paradox patchování

Patchování, nebo také aktualizace, záplatování či opravování, je důležitou součástí správy informačních systémů. Většinou jsou součástí patche funkcionální či bezpečnostní vylepšení a opravy. Z mé zkušenosti běžní uživatelé často odkládají aktualizace svých systémů, dokud samotná aktualizace není systémem vynucená.

Setkávám se s tím, že uživatele aktualizace otravují, kradou jim drahocenný čas. Na jednu stranu se s tímto přístupem dokážu ztotožnit, občas aktualizace také odkládám. Nejedná se však o dobrou praxi a měli bychom aktualizace instalovat pravidelně, dle doporučení výrobce a s vyhodnocením potenciálního dopadu na propojené aplikace.

Ve firemním prostředí, kde administrátoři mají ve své správě desítky, stovky a někdy i tisíce zařízení a systémů, může být patchování opravdová výzva. Přímo se nabízí mít zapnuté automatické aktualizace a tam, kde to není možné, nasadit vhodně nastavené patch management procesy. Běžnou praxí však bývá automatické aktualizace omezovat a raději se držet manuálních zásahů. Proč tomu tak je?

Aktualizace zvyšují použitelnost i bezpečnost, ale mohou snižovat stabilitu. Také patche s sebou mohou nést chyby a někdy je až nemožné vrátit systém po aplikaci špatné aktualizace do původního stavu. Zejména v případě kritických systémů, kdy součástí patche může být přidání či odebrání funkcionality, na které závisí jiné integrované systémy.

Patch management je nutný, jenže ve složitých prostředích může změna vyvolat výpadek,

nekompatibilitu nebo narušení provozu. Oprava zranitelnosti může být tedy současně změnou, která vytvoří novou zranitelnost provozu.

Paradox legacy systémů

V našem oboru se pojmem legacy systém označuje starší software nebo technologická platforma, která je stále v provozu, ale už není moderní podle aktuálních standardů a požadavků. Nejstarší systémy často drží nejdůležitější procesy. Právě proto se jich bojíme dotknout. Nejde však pouze o to, že by systém nebyl aktuální. Legacy systémy jsou z mého pohledu rizikem ze tří hlavních důvodů.

Prvním je to, že jsou často implementované v nějakém zastaralém programovacím jazyku či frameworku. To je významné provozní riziko v případě, že je nutné v systému ladit nějaké chyby či přidávat nové funkcionality. Je pravděpodobné, že v případě potřeby bude obtížné či drahé sehnat člověka, který danou

technologii ovládá. Navíc u podobných případů bývá dokumentace v naprosto nepoužitelném stavu, nebo chybí úplně.

Dalším důvodem je to, že často se jedná o nějaký kritický systém, bez kterého se společnost jen tak neobjede nebo je velmi obtížné ho nahradit. Vidíme to často u výrobních podniků, kde pořizované stroje jsou často nakupovány s životností i několik desítek let. Tyto stroje a jejich integrované části jsou mnohdy jednoúčelové a pracují celou dobu právě v kooperaci s původně navrženým softwarem. Počítačové systémy mají však mnohem kratší životnost a vyžadují pravidelné aktualizace pro zajištění stabilní funkčnosti a bezpečnosti.

Jako třetí zásadní důvod vnímám omezenou či nulovou flexibilitu. Změny ve funkčnosti a integrace na moderní systémy pro zajištění automatizace se stává spíše utopií.

Mohl bych vymyslet deset dalších důvodů, proč jsou legacy systémy významným rizikem. Nicméně výše vybrané tři důvody za mě shrnují to nejdůležitější. Nejstarší systémy bývají největším rizikem a současně nejméně nahraditelné. Legacy prostředí často drží

klíčové procesy a zároveň nejhůře snášejí moderní bezpečnostní opatření.

Paradox cloudu

Cloudové infrastruktury a aplikace jsou dneska naprosto běžnou součástí fungování organizací všech velikostí. Co se však reálně skrývá pod tímto obláčkem? Prakticky jde o server či počítač jako každý jiný, jen je umístěn mimo náš fyzický dosah. Mám na mysli datová centra. Datová centra poskytují prostor, chlazení, záložní energii, zajištění fyzické bezpečnosti. Přejímají na sebe odpovědnost za určitou část provozu a umožňují nám přístup k našim datům a systémům prostřednictvím internetu. Existuje několik typů cloudu, kdy je nám pronajímán například jen výpočetní výkon, konkrétní aplikace, zálohovací prostor a podobně. Mají však vždy jedno společné. Část funkčnosti je nám jako uživatelům a administrátorům skryta.

Bývaly doby, kdy každý administrátor chtěl mít své vlastní železo (hardware) dostupné ve vlastní serverovně a mít nad vším naprostou kontrolu. Tento způsob má své obrovské plusy i významné mínusy, stejně jako cloud. Volbou správného cloudového řešení se minimalizuje naše odpovědnost za fyzickou bezpečnost. Také většina poskytovatelů účtuje poplatky za provoz v cloudu podle reálně spotřebovaných zdrojů, což může být ve výsledku mnohem výhodnější, než investice do vlastního hardwaru. Není to však pravidlem.

Toto přímo také souvisí s tématem škálovatelnosti. Pokud by nám nestačil současný výpočetní výkon na vlastní infrastruktuře, znamenalo by to pravděpodobně investovat do nákupu nového hardware, konfigurace a integrace na již existující systém. V případě cloudu by se jednalo o jednoduché rozšíření služeb, které si pronajímáme. Ani cloud však není ultimátním řešením na všechny problémy. Zejména z důvodu vysokých cen při migraci kompletní infrastruktury do cloudu. Z toho důvodu se dnes často setkáváme s hybridním řešením, kdy část aplikací a infrastruktury stále funguje lokálně a část je migrovaná do cloudu.

Cloud zvyšuje technologickou robustnost, ale zvyšuje i citlivost v případě chybné konfigurace. Mohou se objevit chyby ze strany poskytovatele, které výrazně ovlivní fungování našich systémů a nad kterými máme nulovou kontrolu. Zároveň se pro zjednodušení procesů využitím cloudu vzdáváme určité části kontroly nad daty i systémy. Cloud odstraňuje naše servery z místnosti. Neodstraňuje však odpovědnost za to, co na nich běží.

Paradox konektivity

Je faktem, že velká část byznysu se odehrává online. Přestože v mnohých programech i dnes dokážeme pracovat plnohodnotně v režimu offline, připojení k internetu je pro nás zásadní. Potřebujeme synchronizovat změny, odesílat zprávy a přílohy, připojovat se na aplikace, komunikovat s klienty či s vlastním týmem. Stabilní a rychlé připojení se proto stává kritickou součástí moderního byznysu.

Mohl bych zde popisovat do detailu redundantní síťové linky a jak se zajišťuje stabilní konektivita na úrovni sítě. Nicméně přílišný technický detail není v souladu s tématikou této knihy.

Pokud naše společnost není úplně malá, potřebujeme zajistit přístup k síti i v případě výpadku poskytovatele připojení. Společnosti například využívají více různých poskytovatelů najednou. Na interní síti investují do hardware, který zprostředkovává vhodnou konektivitu mezi interními zařízeními i mezi zdroji jinde v internetu. Máme uvnitř sítě i na její hranici bezpečnostní prvky a systémy zajišťující požadovanou kvalitu připojení.

Zajištění stability a funkčnosti sítě však nestačí. Síť musí být dobře strukturovaná, respektive segmentovaná. Musí být monitorovaná a na incidenty musí být schopna vhodně reagovat. Pokud je síť postavená jen na základním propojení zařízení, může nahrávat do karet také útočníkům. Bezpečnost musí být aplikovaná už při návrhu samotné sítě.

Pokud jsou systémy propojené bez adekvátního zabezpečení, problém se mezi nimi může šířit výrazně rychleji. V nevhodně segmentované síti může i jedno

infikované zařízení znamenat kompromitaci celé společnosti.

Paradox automatizace

V dnešním rychlém byznys světě bych slovo automatizace klidně postavil jako synonymum k termínu konkurenceschopnost. Nemusí to nutně znamenat integraci systémů umělé inteligence. Znamená to eliminaci neefektivních procesů. Zvětšuje se objem dat, které potřebujeme zpracovávat. Zkracují se časové intervaly, za které je nutné mít připravené kvalitní výstupy. V byznys světě je to závod o čas a peníze.

Firmy digitalizují a automatizují. Snaží se zbavovat papírových formulářů všude, kde je to možné. Následně nad digitalizovanými procesy staví systémy, které určité činnosti provádějí za člověka. Vůbec nevadí, pokud občas automat udělá chybu. Naopak by bylo zvláštní, kdyby fungoval bezchybně. Pro odhalení logických chyb by však i v automatizovaném procesu měl

někde figurovat člověk. Například v controllingu a zajištění kvality. Za finální výstup nikdy neodpovídá automat, ale člověk či skupina lidí. Eliminace člověka ze všech procesů by jednoduše mohla vést k propagaci chyby napříč různými systémy. A to bez možnosti jejího odhalení, zhodnocení kontextu a nápravy.

Automatizace omezuje lidské chyby, ale násobí systémové chyby. Když člověk udělá chybu ručně, dopad bývá omezený. Když ji udělá automatizovaný proces, okamžitě ji škáluje.

Paradox šifrování

Šifrování brání cizím očím vidět naše data. Někdy ale brání i našim očím vidět útok. Osobně mám velmi rád šifrování. Jedná se o matematicko-počítačovou disciplínu, jejímž cílem je chránit důvěrnost našich dat. Mnoho lidí žije v mylné představě, že šifrovací mechanismy jsou tady s námi pouze posledních několik let. Opak je pravdou. Už Julius Caesar využíval principy šifrování k zasílání citlivých vojenských zpráv a rozkazů

svým Centurionům. Vedlo to ke vzniku ochrany dnes známé jako Caesarova šifra. Velmi jednoduše – vyberte si slovo a každé písmeno nahraďte písmenem o 3 místa v abecedě dále. Pokud tímto způsobem byla přeložena celá zpráva, byla při odchycení nepřítelem nečitelná. Pouze osoba se znalostí dešifrovacího klíče, tedy posunu každého písmena o tři místa v abecedě zpět, byla schopná zprávu rozluštit.

Od římských dob již uplynulo mnoho času a spousta věcí se změnila. Včetně šifrování. Dnes již využíváme velmi komplexní algoritmy, než pouhý posun znaků o pár míst. Zůstalo však jedno společné. Stále důvěrnost našich dat stojí a padá na utajení šifrovacích a dešifrovacích klíčů. Pokud někdo neoprávněně získá přístup k šifrovacím klíčům, kterými jsou chráněna citlivá data, ani ten nejlepší algoritmus ho nezastaví.

Byly doby, a není to tak dávno, kdy některé části internetu šifrované nebyly. Bylo to proto, že šifrování je výpočetně náročný proces a mohl zpomalovat používání počítačů. V dnešní době, kdy pomalu každý telefon v našich kapsách má mnohonásobný výkon starších počítačů, neexistuje legitimní důvod pro používání nešifrované komunikace.

Šifrování má spoustu výhod a jen málo nevýhod. Útočníci také běžně využívají šifrovacích technologií. Ať už pro skrytí své činnosti či například k ransomwarovým útokům. Ransomware si jednoduše můžeme představit jako úspěšnou infiltraci společnosti a všech jejich systémů, kdy útočník na konci svých činností provedl mimo jiné také zašifrování všech dostupných dat. V takový moment využívá legitimní operace, šifrování, k zajištění „důvěrnosti“ dat, která mu nepatří a stává se jediným, kdo tato data může také rozšifrovat. Výsledkem je vydírání oběti s cílem získat výkupné, tradičně v kryptoměnách, za příslib navrácení dat. Ransomware je velmi zajímavé téma, které by si zasloužilo celou vlastní knihu, ale s ohledem na tématiku této knihy a pro jednoduchost nyní povídání o ransomware ukončím.

Šifrování chrání data, ale může zároveň komplikovat obranu. To, co chrání důvěrnost, může znesnadnit monitoring, forenzní analýzu nebo detekci škodlivé komunikace.

III. Lidé

Dostali jsme se do sekce o lidské stránce bezpečnosti, tedy o důvěře, pohodlí, chování a kultuře. Jsem dlouhodobý zastánce tvrzení, že člověk je nejslabším článkem bezpečnosti organizace, ale vhodně proškolený a pozorný uživatel je mnohonásobně lepší investicí než drahý firewall.

V dnešní době klademe důraz na automatizaci neefektivních procesů a v rámci digitalizace se zbavujeme papírových dokumentů. A dokonce rychleji, než kdy dříve. Do toho všeho vstupuje AI, která dokáže mnohé automatizace ještě více obohatit. Nicméně věřím, že nás autonomní systémy nikdy plně nenahradí. Je však za mě velmi relevantní uvažovat o AI a automatizaci jako o juniorním kolegovi, který dokáže opakovaně a v dobré kvalitně provádět rutinní úkoly v krátkém čase.

V této části popisuji, proč člověk není jen problém, ale také jediný prvek systému, který umí chápat plný kontext. Je to blok o psychologii, motivaci a organizační realitě.

Paradox člověka

V předchozích kapitolách jsem popisoval paradoxy technologií, které tvoří první linii obrany proti kybernetickým hrozbám. Pokud pro útočníka není aktuálně k dispozici cesta k infiltraci systémů skrze technické slabiny, dává z jeho pohledu smysl zaměřit se na lidský faktor. Člověk je nejslabší článek, ale také poslední obranná linie.

Útoky cílící na uživatele obecně označujeme termínem sociální inženýrství. Jedná se o soubor metod a technik, které se snaží manipulovat lidskou psychiku k vykonání nějaké nežádoucí akce. Může se jednat o podvodné e-maily, smsky, hardwarové usb zařízení, koukání přes rameno s cílem odhalit uživatelovo heslo či jen pouhé odposlouchávání konverzací v open office. Útoků na bázi sociálního inženýrství existuje velké množství. Nebudu se zde pouštět do jejich bližšího popisu, jelikož tomuto tématu jsem se detailně věnoval v předchozí knize, Nástrahy internetu.

Paradoxem je, že lidé klikají, chybují a často podlehnou tlaku, vlastní zvědavosti, nepozornosti či falešnému pocitu štěstí. Zároveň jsou jediní, kdo dokáže

plně zachytit kontext, mají intuici a schopnost rozpoznat neobvyklé chování v náročných situacích. Někdo by mi zde mohl oponovat, že AI systémy dnes také vyhodnocují celý kontext útoku. Nemyslím si, že je to pravda. Člověk má stále výhodu propojovat informace z virtuálního, fyzického a sociálního světa a má možnost odhalovat anomálie i tam, kde by dnešní autonomní systémy selhaly.

Paradox pohodlí

Nikdo z nás se nechce stát obětí kybernetického útoku. Dlouhodobě na školeních vtloukávám do hlavy jednotlivcům i společnostem, že každý z nás se může stát obětí kyberkriminality. Nezáleží na tom, jestli jsme fyzická osoba, malý, střední či velký podnik nebo nadnárodní korporace. V každém z těchto případů se dá z pohledu hackera najít atraktivní cíl.

Přestože nikdo z nás nechce být cílem útoku, často záměrně nedodržujeme bezpečnostní procesy.

Nemáme vhodné technologie a nedodržujeme bezpečnostní politiky. Proč tomu tak je? Protože bezpečnost je zásahem do uživatelského komfortu. Samozřejmě záleží na typu, množství a konfiguraci bezpečnostních opatření. Je však pravdou, že každé bezpečnostní opatření uživatele v nějakém směru ovlivňuje. Přestože to třeba přímo nepociťuje.

Může se jednat o zabezpečení koncových zařízení, která omezují možnosti spouštění programů a přizpůsobení systému. Mohou to být monitorovací systémy, které uchovávají informace o činnostech uživatele a dále je vyhodnocují. Mohou to být prvky perimetru organizace, které povolují či zakazují místa, kam se může uživatel do internetu připojovat. A může to být mnoho dalších opatření. Každé z nich může mít přímý vliv na uživatelskou zkušenost – pomalejší odezva systémů, nemožnost vykonat nějakou akci, narušení uživatelské přívětivosti, závislost na IT či bezpečnostním oddělení organizace.

Lidé chtějí bezpečnost, pokud je nic nestojí. Čím více opatření snižuje komfort, tím větší je tendence je obcházet, ignorovat nebo sabotovat.

Paradox důvěry

Možná jste se už setkali s konceptem Zero Trust. Ve zkratce, jedná se o koncept neustálého ověřování zařízení, požadavků a aplikací s cílem zajistit přístup k systémům pouze legitimním účtům. Tento koncept je založen tedy na nedůvěře, opatrnosti a skepsi.

V netechnické části kybersvěta je však takový přístup mnohdy těžké aplikovat. V některých případech dokonce i nemožné. Zejména s ohledem na zaměstnance, kontraktory, klienty a dodavatele.

Konkrétním příkladem může být outsourcing správy firemního IT prostředí od externího dodavatele. Firmy tak získávají tým odborníků, zastupitelnost a množství rizik přenášejí na dodavatele. Aby mohl dodavatel IT prostředí spravovat, je nutné mu poskytnout také administrátorské přístupy do většiny systémů. Můžeme mít vztah krytý smlouvami a různými dodatky. Nicméně nikdy si nemůžeme být naprosto jisti, že se na straně dodavatele vše děje správně a bezpečně. Důvěra je zde naprosto zásadní.

V dnešním světě je už docela běžné, že se pokročilé hrozby, jako například hackerské skupiny,

snaží infiltrovat společnosti mimo jiné přes jejich dodavatele nebo se nechají jednoduše najmout jako plnohodnotní zaměstnanci.

Organizace musí fungovat na důvěře, ale útočníci ji zneužívají jako hlavní vstupní bod. Útoky na bázi sociálního inženýrství či například „insider threats“ stojí na tom, že lidé věří procesům, autoritám a známým vzorcům chování.

Paradox školení

Kontinuální školení zaměstnanců v oblastech kybernetické bezpečnosti je za mě naprosto klíčové. Opakování je matka moudrosti a zde to platí dvojnásobně.

Školení ale nesmí nikdy stát pouze na rutinním vyplnění krátké kvízu jednou ročně. Ještě se stále setkáváme s firmami, kde se k pravidelnému školení zaměstnanců přistupuje jako k nutnému zlu. Něčemu, co se musí splnit, abychom získali zelenou fajfku a falešný

pocit bezpečí. Tento přístup je fatálně špatně. Kromě nulové informační hodnoty pro uživatele se jedná také pouze o pálení času všech zúčastněných. Lidí, kteří školení zajišťují, a všech účastníků, kteří ho musí absolvovat.

Správný přístup zahrnuje živý přednes vybraných témat, demonstraci jejich praktičnosti a realističnosti. Skvělým nástrojem osvěty je také gamifikace, tedy školení hrou. Například formou kvízu, výzvy a úkolů. Smyslem není stupňovat náročnost, ale přimět účastníky, aby se nad tématy zamysleli. Ne je pouze očima prolétli. Je velmi pravděpodobné, že v dnešní době bude spousta uživatelů při řešení úloh spoléhat na internetové zdroje a systémy umělé inteligence. I to je však naprosto v pořádku. Není nutné nikoho dusit nad řešením hlavolamů a úkolů. Naopak, umět si vyhledat informace a ověřovat jejich správnost je jednou z nejdůležitějších schopností moderní digitální doby.

I tahle mince má však své dvě strany. Čím více se o hrozbách mluví, tím snáze lidé otupí. Příliš časté varování může vést k únavě, formálnímu plnění a ignoraci skutečně důležitých signálů.

Paradox motivace

Nikdo z nás netouží stát se cílem kybernetického útoku. Osobní informační bezpečnost v domácím prostředí však stále podceňujeme. Jsou to neustále skloňovaná slabá hesla, osobní počítače a telefony bez koncového zabezpečení či například nezabezpečené domácí wi-fi routery. Přesto zůstávám optimistou a budu tvrdit, že i tyto případy pomalu, ale jistě mizí a lidé si začínají více a více uvědomovat křehkost systémů a hodnotu svého soukromí a bezpečí. Často se mě lidé ptají, jaký antivirus doma používat, jaká hesla jsou bezpečná a jak ona komplexní hesla uchovávat a používat. V rámci diskuze vyjde mnohdy najevo, že buď už se reálně setkali s nějakým útokem na vlastní kůži, nebo se stal terčem útoku někdo, kdo je jim blízký. Motivací pro bezpečnost zde bývá strach z viditelného dopadu na někoho známého nebo sebe sama.

Ve firemním prostředí bývá motivace mnohdy jiná. Lidé neřeší bezpečnost svých zařízení a aplikací. To není náplní jejich běžné práce. Přesto jim bezpečnost není lhostejná. A vlastně ani být nemůže. Ve firemním prostředí je povinností zaměstnanců nahlašovat

podezřelá chování, která by mohla vyústit v incident. Deset hlášení, která se ukáží být falešným poplachem, je mnohem lepší, než jedno nenahlášené podezření, ze kterého se stane reálný incident s významným dopadem. Ve zdravé společnosti s vhodnou bezpečnostní kulturou se zaměstnanci nebojí nahlašovat svá podezření. Motivací zde pak bývá pocit sounáležitosti z reálného přispění k bezpečnosti organizace, ale někdy také strach z toho, že ponesou odpovědnost, pokud podezřelou událost nenahlásí.

Obecně si myslím, že lidé chtějí chránit firmu, ve které pracují. Mnohem důležitější pro ně však je odvést svou práci. Bezpečnost tak bývá v očích uživatelů překážkou pouze tehdy, pokud není navržena tak, aby podporovala jejich reálné cíle.

Paradox únavy

Bezpečnost je vždy zásahem do fungování systémů nebo činností uživatelů. Vhodně vybíraná a nasazovaná řešení však berou faktor člověka vždy v úvahu. Nemělo by docházet k tomu, že bude bezpečnostní opatření významnou překážkou pro vykonávání běžných činností. Pokud by tomu tak bylo, začnou si uživatelé hledat příjemnější cesty k dosažení svého, i kdyby to mělo znamenat vědomé porušování bezpečnostních politik a postupů. Z pohledu bezpečnostního manažera je nutné tedy vždy přemýšlet také nad dopadem zaváděných procesů a technologií na koncové uživatele. Každé bezpečnostní rozhodnutí má svou cenu. Když jich po lidech chceme příliš, začnou platit pozorností.

Krásným příkladem je správa hesel. Když by se mě někdo zeptal, jak má pracovat s hesly, má odpověď bude znít třeba takto. Používat hesla o délce minimálně padesát znaků, využívat číslice, písmena a speciální symboly. Nikdy nepoužívat stejné heslo do více systémů a periodicky si hesla měnit. Zároveň nepoužívat žádné zapamatovatelné fráze. Z pohledu bezpečnosti je toto

správné doporučení, ale pro jeho reálnou použitelnost musí být zahrnuto také zhodnocení lidského faktoru. Jak s takovými hesly efektivně pracovat? Kde je bezpečně ukládat? Jak je vhodně generovat? Odpovědí je správce hesel, který bude všechny tyto činnosti provádět za uživatele. A uživatel se do něj bude přihlašovat například biometrikou. Pak dojde nejen k povýšení bezpečnosti, ale také efektivity práce, protože uživatel hesla nebude muset manuálně opisovat do přihlašovacích formulářů.

Podobných příkladů bych mohl vymyslet několik. Smyslem této kapitoly je však demonstrovat, že přidávání bezpečnostních prvků nemusí nutně umocňovat znechucení uživatelů, pokud se do analýzy potřeb zahrnuje také lidský faktor. Čím více rozhodnutí po lidech bezpečnost vyžaduje, tím horší rozhodnutí dělají. Bezpečnostní prostředí plné výjimek, malicherné byrokracie a schvalování vede k rozhodovací únavě a rutinním chybám.

Paradox odpovědnosti

Bezpečnost byla v organizacích přirozeně vždy až druhotné téma. V první řadě bylo potřeba, aby fungoval byznys. A to, zda funguje bezpečně, se řešilo vždy až poté. Nyní je bezpečnost organizací stejně důležitým pilířem jako jejich provoz. Kvůli tlaku klientů, legislativy a dalším faktorům. Navíc si stále více lídrů uvědomuje, že implementace bezpečnosti již při samotném návrhu procesů a technologií je mnohem efektivnější a levnější, než integrovat tuto fundamentální část do již zaběhlého fungujícího systému.

A zde se dostávám k tématu odpovědnosti. Tu je totiž nutné určovat v každé fázi životního cyklu projektu. Je nutné ji určit u každého aktiva. Může se jednat o zdlouhavý proces, který v danou chvíli nepřináší žádný užitek. Tento proces je však nutný nejen pro správné řízení rizik, ale také pro řešení reálných problémů s danou technologií či procesem. Pokud nevíme, na koho se v krizovou chvíli obrátit, může i jednoduchý problém přerůst v kritický incident s dopadem na fungování celého byznysu.

Často se stává, že z důvodu pohodlnosti se mnohdy vybere jeden obětní beránek, který je připsán jako odpovědná osoba k většině procesů a technologií ve firmě. Sice po formální stránce může podobně vyplněný registr vypadat obstojně, při řešení reálných problémů však nebude nijak nápomocný. Také se setkávám se situacemi, kde onen obětní beránek není jedna osoba, ale skupina osob. Například „IT oddělení“. Takto definovaná odpovědnost za provoz a bezpečnost nějakých aktiv asociuje, že za ni odpovídají všichni z dané skupiny.

A když za bezpečnost odpovídají všichni, často za ni neodpovídá nikdo. Bez jasného vlastnictví tématu vzniká organizační mlha, kde se každý spoléhá, že to řeší někdo jiný. Odpovědnost napsaná v tabulce nevytváří odpovědné jednání. Jen ukazuje, koho budeme hledat, až nastane problém.

Paradox insidera

Ještě stále jsou ve firmách a organizacích potřeba skuteční lidé. Přestože lze dnes spoustu věcí automatizovat a mnoho činností pomáhá zefektivňovat AI, není možné lidský faktor vynechat. Také nevěřím, že někdy nastane doba, kdy by byl člověk stoprocentně nahraditelný. Máme a budeme mít lidi, kteří mají přístupy a práva k interním systémům. Jedná se o zaměstnance, klienty, dodavatele, auditory. Z pohledu bezpečnosti budou tito uživatelé, ale také autonomní systémy, vždy představovat interní hrozbu.

Hrozba insidera je často spojována s nějakým nespokojeným zaměstnancem. S někým, kdo již má legitimní přístupy a z nějakého důvodu by chtěl firmě uškodit. Efektivní, ne však všespásnou, obranou proti takové hrozbě je aplikace principů least privilege, need to know, zero trust a separation of duties.

Least privilege je princip založený na tom, že uživatelé dostávají pouze nejnižší oprávnění, které v danou chvíli potřebují pro výkon své práce. Princip need to know umožňuje přístup pouze k takovým datům, které uživatel aktuálně potřebuje pro svou činnost. Zero

trust je implicitní nedůvěra, která je realizovaná neustálým ověřováním aplikací, požadavků a identit. Separation of duties pak odděluje odpovědnosti tak, aby například schvalovatel změny v systému nemohl tuto změnu sám technicky provést.

V menších nebo nevyzrálých podnicích se tyto principy mnohdy ignorují a velká míra kompetencí zůstává i na jediném člověku. Avšak ti nejdůvěryhodnější lidé mohou představovat největší riziko. Ne kvůli zlému úmyslu, ale kvůli kombinaci přístupu, znalostí a podceňovaného dohledu. Největší interní hrozbou nemusí být člověk, který chce škodit. Někdy je to člověk, kterému věříme natolik, že se ho přestaneme ptát.

Paradox loajality

Útočníci využívají metody sociálního inženýrství pro manipulaci lidské psychiky s cílem vykonat nějakou akci. Může jít o vyzrazení přihlašovacích údajů, spuštění nějaké akce v informačním systém, stažení malware a podobně. Sociální inženýrství je mnohem více, než podvodné e-maily a smsky. Využívají se zde techniky nátlaku, vyvolání pocitu štěstí, strachu, paniky, soucitu. Úspěšnost takového útoku závisí na kreativitě a přesvědčivosti podvodníka.

Častým cílem pokročilých podvodů nejsou administrátoři systémů či bezpečnostní pracovníci. Naopak to budou lidé, u kterých se předpokládá přetíženost a z toho plynoucí nepozornost. Některé reálné útoky na bázi sociálního inženýrství mohou být opravdu zákeřné a cílí na oklamání důvěřivého člověka s cílem mu uškodit. Motivovaný útočník může místo nátlaku zpočátku projevovat naopak snahu o sblížení. Jakmile nalezne něco, co je pro daného člověka osobní či citlivé, zaměří se přímo tam a může onu záležitost použít jako páku pro vytvoření přesvědčivého podvodu. Takové počínání je daleko za hranou běžného testování

zaměstnanců. V tomto případě se podobné techniky a taktiky používají opravdu jen při reálných podvodech nebo pokročilých red teamingových cvičeních.

Loajálnímu zaměstnanci může záležet na tom, aby se práce dotáhla do konce, i kdyby to mělo znamenat nějaký nestandardní postup. Poskytnutí přístupů, propůjčení zařízení, přenos dat skrze nezabezpečené úložiště či neznámá USB zařízení. Proto i loajální zaměstnanec může být pro útočníka cennější než nespokojený insider. Útočníci často raději zneužijí ochotného, pracovitého a důvěřivého člověka než někoho, kdo se otevřeně staví proti firmě. Loajalita drží organizaci pohromadě. A právě proto ji lze zneužít k tomu, aby někdo obešel pravidla ve jménu dobrého úmyslu.

Paradox expertízy

Nikdo z nás se expertem nerodí. Musíme si svou cestičku prošlapat sami. Od studia základních principů přes pokročilá témata a řešení dílčích problémů až po strategická rozhodnutí. Je naprosto přirozené, že součástí týmů jsou junioři, budoucí experti. Mít tým složený pouze ze seniorních expertů mnohdy nedává smysl, například z finančních, časových a kapacitních důvodů. Zároveň chceme mít k dispozici v týmech senioní experty, kteří budou využívat své know-how k zajišťování kvality projektů a vedení juniornějších kolegů.

Člověk není tvor bezchybný. Stejně tak jako každý z nás, i ten největší expert v oboru může udělat chybu. Paradoxem je, že čím zkušenější expert, tím je vyšší dopad jeho chyby. Znalosti zvyšují kvalitu práce, ale také rozsah oprávnění a důvěry. Chyba seniorního admina nebo architekta bývá zásadnější než chyba juniora. Expert má moc řešit věci, které jiní nevyřeší. Stejná moc dává jeho omylu větší dosah.

Paradox kompetence

Organizace obecně směřují k vyšší efektivitě. Cílem je udělat stejné množství práce za kratší čas, s menším počtem lidí a s nižšími náklady. To už není sci-fi ani vzdálená představa budoucnosti. Je to každodenní realita kybersvěta, ve kterém rutinní úkoly stále častěji přebírají automatizované systémy a AI agenti.

Na první pohled se zdá, že jde o přirozený pokrok. Stroje zvládají opakující se činnosti rychleji, levněji a bez únavy. Člověk se tak může věnovat složitějším rozhodnutím, strategii a tvořivé práci. Jenže právě zde vzniká paradox. Čím více práce přenecháváme umělé inteligenci, tím méně lidí si uchovává schopnost danou práci skutečně vykonat.

Problém tedy nespočívá pouze v tom, že by na trhu nebylo dost pracovníků. Skutečnou výzvou je najít lidi, kteří rozumějí systému do hloubky, nespoléhají se výhradně na nástroje a dokážou řešit komplexní problémy i ve chvíli, kdy automatizace selže. Kompetence se tím stává vzácnější než samotná pracovní kapacita. V kyberbezpečnosti je tento problém obzvlášť výrazný. Moderní digitální infrastruktura je složitá,

propojená a často závislá na technologiích, kterým rozumí jen úzká skupina specialistů. Systémy se vyvíjejí rychleji než lidé, kteří je mají chápat, spravovat a chránit.

Co se stane, když nastane chyba v systému, který už nikdo plně nechápe? Co když AI nástroj nedokáže problém vyřešit, protože situace přesahuje jeho model, data nebo oprávnění? A co když je chyba přímo v samotném AI nástroji, na který organizace spoléhá jako na poslední instanci?

Paradox kompetence spočívá také v tom, že organizace zavádějí automatizaci, aby snížily závislost na lidech, ale zároveň tím zvyšují závislost na stále menším počtu skutečně kvalifikovaných odborníků. Čím více se systém opírá o automatizaci, tím nebezpečnější je okamžik, kdy automatizace přestane fungovat. A čím méně lidí si udržuje praktické znalosti, tím obtížnější je takový okamžik zvládnout.

Organizace, které se příliš spoléhají na úzkou skupinu specialistů nebo na systémy řízené umělou inteligencí, se mohou stát výkonnějšími. Zároveň se však stávají křehčími. Kompetence se pak neprojevuje ve chvíli, kdy vše funguje, ale ve chvíli, kdy se systém rozpadá, nástroje mlčí a někdo musí pochopit, co se skutečně stalo.

IV. Governance

Neustálý tlak na zvyšování kybernetické odolnosti organizací je důsledkem mnoha faktorů. Jsou to legislativní změny, vznik nových regulací, směrnic, standardů. Jsou to stále aktuální hrozby pokročilých kybernetických útoků a v neposlední řadě, jsou to běžně a dlouhodobě zanedbávaná základní bezpečnostní pravidla. Tyto faktory mají společnou jednu velmi důležitou věc. A to, že bez podpory vedení se změny v bezpečnostních technologiích a procesech dají implementovat jen velmi těžko. Pokud vůbec.

Governance je řízení kybernetické bezpečnosti na strategické úrovni. Je důležité si uvědomovat, že se jedná o kritickou součást, bez které se nové technologie a procesy implementovat ve společnosti nedají. Bez podpory leadershipu bude chybět prvek schvalování na úrovni vedení a bez tohoto prvku nebude možné zajistit například financování, součinnost interních týmů a dodavatelů nebo třeba vymahatelnost pravidel vůči zaměstnancům. Governance má vytvořit pořádek. Právě

v pořádku ale může vzniknout falešný pocit, že riziko už je vyřešené.

Toto je sekce o řízení, odpovědnosti, prioritách a rozhodování pod tlakem. Ukazuje, že kyberbezpečnost není jen věcí techniků, ale především leadershipu, governance a schopnosti dělat kvalitní rozhodnutí v nejistotě. Je to blok o tom, kdo nese odpovědnost, jak se riziko komunikuje a proč formální splnění pravidel nestačí.

Paradox strategie

Bezpečnost je velmi důležitou součástí strategie organizací. Sama o sobě však není na jejím vrcholu. Nejdříve je nutné uvažovat, co bude předmětem byznysu, na koho budeme cílit a jak budeme svou činnost vykonávat. Až poté potřebujeme řešit, že plánovaný byznys budeme realizovat s ohledem na vlastní bezpečnost a bezpečnost našich partnerů. Zní to tedy, že z pohledu strategie je bezpečnost až na druhém místě. Paradoxně musí být však součástí plánování všech

dílčích aktivit, tedy i těch na prvních místech v žebříčku priorit. Z pohledu strategie je nejvhodnější pohlížet na bezpečnost nikoli jako na samostatný proces, ale jako na nezbytnou část všech procesů.

Bezpečnost je podpora pro fungování byznysu. Její absence v kterékoli části životního cyklu může znamenat významné narušení kontinuity činností. Ze strategického pohledu je nutné na rizika pohlížet v širším záběru a uvažovat, jak by narušení jednoho systému mohlo negativně ovlivnit chod celé společnosti. Proto bezpečnostní procesy fungují také jako záchranná brzda, která má upozornit na strategická rizika. A to i v případě, že operativní rozhodnutí se může zdát jediné smysluplné a správné.

Konkrétním příkladem je v dnešní době stále se zvyšující tlak na implementaci AI nástrojů. Firmy chtějí inovovat a získávat konkurenční výhodu. Bezpečnost však často není zahrnuta do všech vývojových a testovacích procedur. Zneužití nějaké opomenuté zranitelnosti může vést k úniku citlivých informací. Takový únik může vést k sankcím a ke ztrátě důvěry ze strany klientů či partnerů. Najednou má opomenutý technický nedostatek reálný dopad na strategii byznysu.

Bezpečnost má podporovat byznys, ale někdy ho musí brzdit. Bezpečnost není samoúčelná. Přesto nastávají chvíle, kdy musí říct ne, zpomalit produkt nebo odmítnout rizikový krok.

Paradox boardu

Board nemusí znát každý technický detail. Přesto musí nést odpovědnost za rozhodnutí, která se v technických detailech mohou zlomit. Musí činit rozhodnutí, která nejsou jednoduchá a často mají významný finanční dopad. Přesto v tom nejsou sami a mají k dispozici experty v jednotlivých oblastech. Často CIO, IT ředitele, který je odpovědný za provoz. Společnosti již začínají rozumět tomu, že je nutné oddělit odpovědnosti za provoz od odpovědnosti za bezpečnost. Vyzrálejší společnosti proto angažují také CISO, ředitele informační bezpečnosti, nebo CSO, ředitele bezpečnosti.

Již v dnešní době se setkáváme s tím, že u velkých organizací se tito odborní ředitelé stávají stálou součástí boardu. Není to ale ještě standardní praxí. Avšak i tyto

jednotlivé případy ukazují určitý pozitivní trend a to, že se bezpečnost dostává do okruhu nejdůležitějších témat společnosti, která se řeší na úrovni nejvyšších orgánů.

Paradoxem je, že vedení nese odpovědnost za riziko, kterému často technicky nerozumí. Board musí rozhodovat o tématu, které je komplexní, rychle se mění a nedá se zjednodušit na několik ukazatelů v dashboardu.

Paradox metrik

Sledování metrik v oblasti kybernetické bezpečnosti je velmi důležitou součástí. Ještě důležitější je však jejich správná definice. Když lidé hovoří o metrikách, často zmiňují termín KPI. V bezpečnosti jsou však důležitější KRI. Co tyto pojmy znamenají a jaký je jejich vztah?

KPI (Key Performance Indicators) jsou klíčové ukazatele výkonnosti. KRI (Key Risk Indicators) jsou klíčové ukazatele míry rizika. Zatímco KPI odpovídají na

otázku „Jak dobře fungujeme?“, KRI odpovídají na otázku „Jak moc jsme ohroženi“?“.

Konkrétním příkladem KPI může být vysoká míra nasazení více-faktorového ověřování uživatelů. To přímo ovlivňuje KRI ukazující nízkou míru rizika kompromitace uživatelských účtů. Vztah mezi těmito metrikami je tedy takový, že KPI ovlivňuje KRI. V tomto konkrétním případě pozitivně. KPI ukazují, zda bezpečnost funguje efektivně, a KRI ukazují, zda to skutečně snižuje riziko. Přestože jsou oba pohledy důležité, v praxi je pro moderního CSO/CISO obvykle důležitější řídit a komunikovat riziko, tedy KRI.

Board většinou nezajímá počet alertů, ale komplexnější pohledy jako je business exposure, pravděpodobnost incidentu, regulatory impact nebo vykreslení trendu rizika v čase. To, co jde snadno měřit, nebývá to nejdůležitější. Počet alertů, patch rate nebo phishing score vypadají dobře v reportu, ale nemusí vypovídat o reálné odolnosti organizace. Měření má přinášet jistotu. Špatná metrika ale dokáže vytvořit jistotu tam, kde žádná není.

Paradox reportingu

„Kvalita, která není vhodně komunikována, neexistuje.“ Tato věta vzešla z úst bezpečnostního ředitele jedné z předních českých telekomunikačních společností. Bylo to na konferenci zaměřené na témata fyzické i informační bezpečnosti. Ačkoli je tento citát aplikovatelný také v rovině vůči zaměstnancům, zaměřím se na jeho využití s ohledem na reporting vůči vedení společností.

Vedení potřebuje přesná a vhodně interpretovaná data pro provádění kvalitních strategických rozhodnutí. Nicméně přílišný technický detail často není žádoucí. Mnohem cennější pro vedení jsou agregované statistiky, které ukazují bezpečnostní trendy. Pro vedení je mnohem cennější vidět trend účinnosti bezpečnostních školení zaměstnanců, než konkrétní čísla ukazující kolik lidí kliklo na testovací phishingovou kampaň. V tomto konkrétním případě by správný přístup měl zahrnovat vyhodnocení rozkliknutích zpráv s ohledem na počet nahlášených bezpečnostních událostí a třeba množství opakovaně neúspěšných uživatelů. I takto zpracovaná statistika však

může být v očích vedení „příliš složitá“, a proto musí být reporting vždy prováděn na míru společnosti a lidem, kterým je report určen. Bez přizpůsobení cílovému publiku se z reportingu stane pouze další statistika pro statistiku.

Čím stručnější report pro vedení, tím větší riziko zkreslení. Management potřebuje zjednodušení, ale přílišná redukce může skrýt podstatu hrozby nebo falešně uklidnit. Report má zjednodušit realitu. Když ji zjednoduší příliš, začne ji nahrazovat.

Paradox rozpočtu

Investice do bezpečnosti organizace není od toho, aby výhledově generovala zisk. Je důležitá proto, aby organizace mohla svou činnost vůbec provozovat. Z pohledu statutárních orgánů je nutné si uvědomit, že se nejedná o volitelnou složku fungování firmy, nýbrž o jednu z naprosto nezbytných.

Setkal jsem se s mnoha případy, kdy se firma stala obětí ransomware útoku a naším úkolem bylo pomoci minimalizovat škody. V případě existence neporušených záloh pomoci s obnovou, následným zabezpečením celé infrastruktury a aplikací tak, aby se incident ideálně neopakoval.

Bohužel si vedení společnosti uvědomuje reálnost své zranitelnosti příliš pozdě. Počítače jsou po úspěšném útoku nepoužitelné, data nedostupná, komunikace odříznutá. Zaměstnanci nemohou pracovat, klienti nemohou být obsloužení, výrobní linky stojí a pro firmu se svět na chvíli zastavil. Bývá pozdě, když si konečně uvědomí, že taxametr stále běží a i přes aktuální nedostupnost bude muset řešit výplaty, naplňování závazků, dodací lhůty a další povinnosti či výdaje. Někdo by si mohl říct, že to pokryje pojištění proti kybernetickým hrozbám. Pokud ho společnost opravdu má, tak bude muset před čerpáním plnění pojišťovně nejdříve prokázat nezanedbání řízení bezpečnosti. Což bývá velký problém.

Výdaje spjaté s řešením reálného kybernetického incidentu se mohou vyšplhat velmi vysoko. V mnoha ohledech dokážou předčít investice do preventivních opatření a kontinuálního řízení kybernetické

bezpečnosti. Bezpečnost je drahá, dokud nepřijde incident. Pak je levná. Investice do prevence se obhajují hůř než náklady po skutečném selhání. Přesto rozhodují o tom, jak hluboký dopad incident bude mít.

Paradox vlastnictví rizika

Troufám si tvrdit, že princip oddělení povinností, v překladu separation of duties, se ve středních a velkých organizacích obecně uplatňuje velmi často. Dobrým příkladem může být model, kdy obchod zajistí klienta, právník zkontroluje smlouvu, zaměstnanec zadává své výkony, manažer schvaluje, finanční oddělení fakturuje a ředitel garantuje kvalitu. V oblasti IT a bezpečnosti je aplikace tohoto principu také velmi důležitá, mnohdy se však přehlíží nebo upozaďuje s ohledem na zvyšující se objem procesních a bezpečnostních výjimek.

Je velmi důležité, aby bezpečnost nebyla pouhou součástí provozu, ale měla nezávislé postavení, vlastní pohled a jasné kompetence v oblastech, za které

odpovídá. Přestože IT a Security jsou nezávislé entity uvnitř firmy, předpokládá se jejich úzká spolupráce. V moderní firmě mají oba týmy své místo, vzájemně se doplňují. S jejich nezávislými pohledy na různá rizika spjatá se stejnými systémy vzniká řízení bezpečnosti.

IT spravuje systémy a garantuje provoz. Bezpečnostní tým řídí ochranu. Business nese následky. Kybernetické riziko prochází napříč organizací a málokdy respektuje interní hranice kompetencí. Riziko má vlastníka na papíře. Dopad má vlastníka v realitě.

Paradox transparentnosti

Důvěra mezi lidmi ve firmě je zásadní. A neplatí to pouze na úrovni vedení, ale také mezi běžnými zaměstnanci. Tato důvěra obnáší nejen umění komunikace a ochotu spolupracovat, ale také sdílení informací. Tedy transparentnost.

Nelze však všechno sdílet se všemi a je důležité vyhodnocovat rizika spjatá s lidským faktorem. Je nutné

dopředu přemýšlet nad tím, že lidé přicházejí a odcházejí. Že mluví o práci i ve svém osobním životě. Že mohou mít své vlastní zájmy. Obecně hovoříme o tzv. „interní hrozbě“. Nedá se eliminovat a je náročné ji kontrolovat. Nejlepší obranou je motivovaný, důvěryhodný zaměstnanec, kterého práce baví, vidí v ní smysl a pracuje ve vyhovujícím prostředí, včetně kolektivu. Sehnat takového člověka a zařídit adekvátní prostředí není lehký úkol, není to však ani utopie.

Pro běžná prostředí máme k dispozici různé bezpečnostní principy. Jedním z nich je již dříve zmiňovaný přístup „need to know“, tedy povolení přístupu pouze k těm informacím, které daný člověk potřebuje v danou chvíli pro vykonání nutných činností a nic navíc. Existují nástroje, jak tento princip technicky realizovat a přitom zajistit transparentnost i auditovatelnost.

Organizace potřebují sdílet informace, ale každé sdílení rozšiřuje riziko. Bez otevřenosti není spolupráce, bez omezení sdílení není ochrana.

V. Budoucnost

Osobně se velmi těším, co nám budoucnost přinese. Již dnes můžeme vidět obrovské technologické inovace, nad kterými bychom ještě před pár lety mávli rukou s tvrzením, že se jedná o sci-fi. Jsou to autonomní vozidla a drony, systémy umělé inteligence, kvantové počítače a spousta dalších fenoménů. Neustále jako lidstvo posouváme hranice toho, co je v našich silách dosažitelné a jdeme si přímo za tím.

Také jsem velmi zvědavý, jaké úžasné věci a komplexní problémy budou řešit naše děti. Jejich svět bude jiný než ten náš. Děti dnes vyrůstají a budou vyrůstat s pokročilými technologiemi na dosah ruky od útlého věku. Nemyslím si, že je to špatně. Je to naopak velká příležitost oprostit se od rutinních činností a směřovat k poznávání věcí a jevů, o kterých teď třeba ani netušíme, že jsou nám k dispozici k bádání. Nesmíme však usnout na vavřínech. Musíme naší budoucnosti, našim nástupcům a dětem v tomto směru pomáhat

zvládat problémy, které jsme jim svými rozhodnutími připravili.

Digitální svět se vyvíjí rychleji než jakákoli předchozí technologická éra. Nové technologie přinášejí obrovský potenciál, ale také zcela nové typy hrozeb, které jsme ještě nedávno neuměli ani pojmenovat. Paradoxy této kapitoly ukazují, že budoucnost kybernetické bezpečnosti nebude jen o lepších nástrojích – bude především o pochopení hlubších souvislostí mezi technologií, lidmi a důvěrou.

Paradox umělé inteligence

Říká se, že oheň je dobrý sluha, ale zlý pán. Podle mého názoru by se podobná analogie dala aplikovat také na systémy umělé inteligence. Ty jsou nám v mnoha ohledech ku pomoci. Umí generovat text, obrázky, kód. Dokáží se učit, dělat rozhodnutí a pracovat v kontextu informací. Nejspíš nastane doba, kdy v určitých procesech člověka nahradí. Zůstávám však na straně

skepse a věřím, že nikdy nenahradí člověka plnohodnotně.

Nesmíme AI systémům plně důvěřovat. Jejich funkčnost není dokonalá. Umí halucinovat a zkreslovat výsledky. Stejně jako člověk mohou chybovat. Aplikace využívající chytré funkce jsou běžně také náchylné na zranitelnosti, které mohou útočníci zneužívat. O to křehčí systémy bývají, když dochází ke komplexním integracím různých aplikací. Přestože nám mohou mnoho věcí usnadnit a urychlit. Musíme mít ale stále na paměti, že finální odpovědnost za kvalitu výsledků a bezpečnost zpracovávaných dat vždy nese člověk.

Také je nutné si uvědomit, že stejné nástroje pro podporu kreativity a produktivity využívají i útočníci. V dnešní době pokročilých překladačů a dechberoucích grafických generátorů již neplatí, že podvodnou zprávu poznáme dle překlepů v textu nebo špatné grafiky. Tato doba dávno pominula, pokud vůbec někdy existovala. Cílené podvody bývají dnes dokonalými kopiemi originálů. U pokročilých podvodných kampaní, které jsou směřovány na jednotlivce a ne masy uživatelů, mají detekční problémy také moderní bezpečnostní opatření. A to i v případě, že mají k dispozici umělý mozek.

Umělá inteligence posiluje obranu – a zároveň posiluje útočníky. AI nástroje dokáží analyzovat obrovské množství dat, detekovat anomálie a automatizovat obranu. Stejné technologie však umožňují útočníkům vytvářet přesvědčivější phishing, automatizovat průzkum infrastruktury nebo generovat škodlivý kód.

Paradox identity

Firmy běžně využívají desítky až stovky různých aplikací a systémů. Od účetních a jiných kancelářských aplikací přes komunikační platformy až po bezpečnostní technologie. Navíc firmy chtějí inovovat a být konkurenceschopné. Proto vyhledávají neustále nová či optimalizovaná řešení. Kdyby do každého systému měli uživatelé využívat unikátní jméno a heslo, v dlouhodobém horizontu by tento design byl neudržitelný. Proto se využívají systémy IAM – Identity

and Access Management, v překladu systémy pro řízení přístupů.

Ve zkratce, IAM obstarávají správu uživatelských identit a poskytují přihlašovaní do propojených systémů. Uživatel pak má jeden účet, který má být vhodně zabezpečen a tímto účtem se přihlašuje ke všem firemním aplikacím. Kromě přihlašování, tedy autentizace, poskytují také běžně funkci autorizace. Princip autorizace zajišťuje, že dříve autentizovaný uživatel má či nemá mít přístup k té či oné aplikaci nebo specifickým datům.

Každé řešení má svá pro a proti. V tomto případě ono „proti“ je potenciální křehkost centralizovaného řízení identit. Zejména pokud IAM sám o sobě není vhodně zabezpečen nebo v něm existují jiné bezpečnostní díry. Například nedostatečné zabezpečení privilegovaných účtů či sdílení administrátorských práv k samotnému IAM.

Digitální identita je nejdůležitější kontrolní bod a zároveň nejslabší cíl útoku. Moderní bezpečnostní architektury se stále více soustředí na řízení identity. Proto na ni útočníci cílí, ať už krádeží přístupových údajů, obcházením multifaktorového ověřování MFA nebo dalšími metodami na bázi sociálního inženýrství.

Identita má být klíčem k bezpečnosti. Čím více dveří odemyká, tím cennější je její kompromitace.

Paradox integrace

Již několikrát jsem v této knize naznačil, že společnosti běžně používají mnoho různých systémů. Nyní pomineme potenciální bezpečnostní nedostatky každého z nich a zaměříme se na mě jako celek.

Systémy se integrují skrze aplikační rozhraní, kterým se obecně říká API. Tato zkratka znamená Application Programming Interface a je to hojně využívané řešení pro přenos dat mezi různými systémy. Může mít mnoho podob. Principiálně jde o výměnu surových dat bez dodatečného grafického rozhraní pro uživatele. Tato rozhraní jsou přizpůsobená pro využití ve zdrojovém kódu a entitách, které běží na pozadí aplikací. Standardním uživatelům jsou skryta.

Využívají se pro přenos dat nutných pro autentizaci a autorizaci. Využívají se pro přenos

firemních i privátních dat. Využívají je platební brány, bankovní instituce i bezpečnostní řešení. Troufám si říci, že v každé větší aplikaci nalezneme nějakou formu možnosti integrace na další systémy skrze API. Využívání samotného API problém není. Problémem se stává jeho nedostatečné zabezpečení při zpracovávání dat a způsob přístupu k nim.

Čím více jsou systémy propojené, tím hlubší je dopad jediného selhání. Moderní infrastruktura je extrémně propojená – mezi firmami, dodavateli i cloudovými službami. Incident v jedné části ekosystému tak může způsobit domino efekt napříč organizacemi.

Paradox odolnosti

Odolná organizace není ta, která nikdy nespadne. Je to ta, která ví, jak vstát dřív, než pád rozhodne za ni. Ten, kdo si myslí, že se nemůže stát cílem kybernetického útoku, se velice plete. Platí to pro jednotlivce, soukromé firmy i veřejný sektor. Ten, kdo hlasitě tvrdí, že není

třeba dodatečných bezpečnostních opatření, protože útok nikdy nezaznamenal, možná ani netuší, že útočník je již dlouhou dobu infiltrován v síti. Ten, kdo nehodlá investovat do vlastní bezpečnosti, protože „do teď se nám nic nestalo“, si koleduje o problém. Myslet si, že se nacházíme v ultimátní bezpečnosti je velice bláhové.

Naopak bychom měli vždy předpokládat, že k incidentu může dojít právě dnes. A opět to platí pro osobní i firemní život. Jak se budu bránit, když dnes detekujeme hackera v naší síti? Mám dostatečně zálohovaná data pro případ, že přestanou fungovat počítače a servery? Co budu dělat, když mi shoří serverovna? Jak nahradím potenciální výpadek kritické aplikace či dodavatele? Jak odhalím a zabráním exfiltraci velmi citlivých dat ze společnosti? Jak budu řešit incident, kdy skrze mou síť bude infiltrována jiná firma? Co když bude mít kybernetický incident drahé právní dohry?

Podobných otázek se dá vymyslet nespočet a všechny souvisejí se stejným tématem – s řízením rizik. Správně nastavený proces řízení rizik není pouhou formalitou, ale nutnou součástí zvyšování odolnosti firmy. V rámci řízení rizik je velmi vhodné připravovat detailní plány pro podporu kontinuity podnikání a plány

reakce na různé živelné i člověkem způsobené pohromy.

Budoucnost bezpečnosti není o zabránění útokům, ale o schopnosti je přežít. S rostoucí komplexitou je nemožné zabránit všem incidentům. Organizace proto musí přejít od modelu absolutní prevence k modelu resilience, tedy schopnosti rychle detekovat problém a obnovit provoz.

Paradox soukromí

Soukromí vnímám jako jedno z nejdůležitějších práv člověka. Stále častěji se ho však velmi lacině zbavujeme. Asi je to trendem moderní doby, kdy chtíč po uznání cizích lidí za sdílení fotek a videí z vlastního života je cennější než soukromí samotné.

Již v předchozí knize jsem popisoval pohled na to, jak sdílení zážitků může být nebezpečné. A nejen pro nás, ale i pro naše blízké. Zejména pro děti, jejichž nadšení rodiče sdílejí bezhlavě radostné i neradostné chvíle bez domýšlení důsledků. Cokoliv, co umístíme na

internet, tam už navždy zůstane. Může to ovlivnit životy nás i našich blízkých i za dlouhou řadu let.

Nejsem proti sdílení. Naopak jsem velký zastánce otevřenosti a přístupu k informacím. Jako problém však vnímám neuvážené sdílení osobních informací. Dnešní doba nám umožňuje velmi jednoduchý a rychlý přístup k informacím všeho druhu prostřednictvím internetu. Je to dobře nebo špatně?

Internet je pouhý nástroj. Za obsah, který mu dodáme a zveřejníme světu, máme odpovědnost my sami. Technologie dávají lidem více nástrojů k ochraně soukromí, ale také více způsobů, jak ho ztratit. Digitální služby nabízejí anonymizaci, šifrování a ochranu identity. Současně však sbírají obrovské množství dat o chování uživatelů.

Paradox autonomie

V dnešní době je autonomie velmi úzce spjatá s využíváním AI. Zvyšování nezávislosti na některých druzích dodavatelů, zlevňování interních zdrojů, konkurenční výhoda a efektivita práce. To je pouze malý výčet z hnacích sil zvyšování autonomie organizací. Vývoj, nebo spíše prototypování nových systémů, nabral vysoké tempo. S pokročilými modely pro programování může začít s vývojem nových systémů téměř kdokoliv. Bez znalosti principů návrhových modelů a bezpečnostních prvků však tyto systémy představují v rukou nezkušeného vývojáře velké riziko.

S autonomií procesů a systémů se pojí jejich vývoj na míru potřeb organizace. Dále pak digitalizace zastaralých procesů a automatizace rutinních činností. Pokud jsou tyto systémy a procesy provozovány a spravovány vhodným způsobem, efektivita a zisky organizace nejspíše jenom porostou. Co když ale vše zautomatizujeme a nastane nějaká neočekávaná událost? Co když bude nutné upravit chod automatizace či zpracovávaná data? Co když bude nutné řešit funkcionální nebo bezpečnostní nedostatky? Co když

budeme chtít automatizace rozšířit nebo minimalizovat? Budeme mít na tyto činnosti kompetentní zdroje? Budou tyto kompetentní zdroje, lidé, schopni vyřešit problém i bez podpory AI, která sama o sobě může být příčinou onoho problému? Autonomie snižuje potřebu zásahu člověka. A tím zvyšuje cenu okamžiku, kdy člověk zasáhnout musí.

Čím autonomnější budou systémy, tím obtížnější bude určit odpovědnost za jejich chyby. Autonomní systémy a AI rozhodování mohou fungovat bez přímého lidského zásahu. Pokud však způsobí škodu nebo bezpečnostní incident, vyvstává otázka, kdo je skutečně odpovědný.

Paradox autenticity

Kvalita pro mě osobně bude vždy důležitější než kvantita. Přesnost hodnotnější než odhad. Autenticita cennější než padělek. Různé zdroje se v konkrétních číslech často rozcházejí, ale obecně se odhaduje, že více

než polovinu veškerého obsahu na internetu negenerují lidé, ale automatizované systémy a boti. Zhruba polovina z tohoto množství je pak podvodným či škodlivým obsahem.

Nejen s příchodem AI systémů se tento trend ještě urychlil. A nejde pouze o kvantitu, ale také o kvalitu. Dnešní podvody jsou mnohdy naprosto nerozpoznatelné od originálů. Týká se to textových zdrojů, obrázků, videí, aplikací i uživatelských identit. S těmito podvody se nejčastěji setkáváme na sociálních sítích. Tam se falešné profily s různými úmysly běžně propagují skrze počítačem generovaný obsah.

Jak tedy v dnešní době rozpoznat podvrh? Jste si stoprocentně jistí svou schopností rozpoznávat podvrhy? Sám si nemyslím, že bych rozpoznal všechny kvalitně provedené cílené podvody. Proto i při běžném brouzdání internetem kladu větší důraz na kvalitu než na kvantitu. Pozorně kontroluji adresy odesílatelů a url adresy webů. Snažím se vyvarovat přímých kontaktů s neznámými osobami, zejména pokud cítím úmysl přesměrovat mě na nějaký web či stažení souboru. Naše lidské kritické myšlení zůstává naší nejefektivnější obranou. Také je naší efektivní zbraní pro rozpoznání autenticity.

Čím snazší je vytvořit digitální podvrh, tím cennější je skutečná autenticita. Deepfakes, syntetické identity a generativní AI zpochybňují samotnou důvěru v digitální obsah. Budoucnost bezpečnosti bude stále více o ověřování pravosti.

Paradox kvantové budoucnosti

Kvantové počítače byly dlouho považovány za výmysl ze sci-fi filmů. Tuto technologii budoucnosti mají však výzkumníci k dispozici již dnes. Dokonce i u nás v České republice. Ještě bude nějakou dobu trvat, než budou průmyslově využitelné, zejména kvůli své vysoké nestabilitě a provozu možném pouze při teplotách blízkých absolutní nule.

Aktuální stav na poli kvantových počítačů mi velice připomíná stav standardních počítačů v 50. letech dvacátého století. Tehdejší sálové počítače o velikosti nákladních automobilů by se mohly jen těžko porovnávat s výkonem dnešních chytrých hodinek. Jako lidstvo jsme

dokázali miniaturizovat obrovský výkon do kompaktních rozměrů. Zařízení s tímto výkonem nosíme denně po kapsách. Věřím, že s kvantovými počítači to bude podobné.

Nějakou dobu bude trvat, než se stanou stabilním nástrojem výzkumu a provozu. Z pohledu kybernetické bezpečnosti bychom se však na tu dobu měli začít připravovat už nyní. A to i v případě, kdy by se ukázalo, že stabilní kvantový počítač zkrátka není možné vyrobit. Opět to souvisí s řízením rizik. Kvantové počítače jsou navrženy pro řešení extrémně komplexních úloh, na které dnešní superpočítače nestačí. Jedná se o simulace katastrof, vývoj nových léků a materiálů, optimalizace logistiky a spoustu dalších. Ono riziko spočívá v prolomení dnešních bezpečnostních mechanismů, jako například asymetrické kryptografie. Ta chrání především důvěrnost dat. Problém narušení tajných dat může mít velké následky pro firmy i státy. A to dokonce i v případě, že k takovému odtajnění dojde u dat a informací starých desítky let.

Technologie, které dnes chrání data, mohou být zítra prolomeny technologiemi novými. Vývoj kvantového počítání může v budoucnu ohrozit současné kryptografické algoritmy. Data, která jsou dnes

bezpečná, mohou být zítra zranitelná. To, co dnes ukládáme jako tajné, může být zítra čitelné. Bezpečnost dat se tedy rozhoduje dlouho před tím, než samotné riziko dozraje.

Paradox predikce

Statistika nuda je, má však cenné údaje. Díky sběru dat a jejich vyhodnocování jsme schopni předpovídat budoucí vývoj různých jevů. Můžeme využívat sofistikované matematické modely, moderní software i mozek umělé inteligence. Vždy však bude platit, že predikce je pouze kvalifikovaný odhad. Ten se může i nemusí naplnit. Může být velmi blízký realitě a zároveň může být naprosto špatný.

V kybernetické bezpečnosti stavíme předpovědi na základě známých hrozeb, minulých incidentů a identifikovaných zranitelností. Těžko se však predikují situace založené na nedostatcích a chybách z neznámého. Paradoxní také je, že v průběhu

posledních desetiletí velké vývojářské firmy investovaly spoustu financí do vývoje a testování svých produktů. Přesto jsou i dnes objevovány zranitelnosti těchto systémů, které ovlivňují chod integrovaných aplikací a mohou mít neblahý vliv na fungování celých společností.

Čím více se snažíme předvídat budoucí hrozby, tím častěji nás překvapí ty nečekané. Bezpečnostní strategie jsou založeny na analýze známých scénářů. Skutečné incidenty však často přicházejí z nečekaných kombinací technologií a lidského chování. Predikce uklidňuje, protože pracuje s daty. Překvapení přichází právě tam, kde data neměla co říct.

Paradox budoucnosti

Trend budoucnosti v oblasti firemního IT je jasný. Chceme efektivní systémy, které budou podporou produktivity a budou nám šetřit čas a peníze. Budou mít přívětivé uživatelské rozhraní a práce s nimi nebude omezena na konkrétní zařízení, místo nebo čas.

Z pohledu bezpečnosti je cíl také jednoznačný. Chceme, aby ani systémy, ani lidé nebyli existenční hrozbou pro společnost. Aby firmy mohly své činnosti vykonávat bezpečně a s důvěrou ve vlastní prostředí. Chceme mít k dispozici tak dobrá bezpečnostní opatření, aby třeba pouhé otevření podvodné stránky nemohlo mít kritický dopad. Chceme mít tak dobrá bezpečnostní opatření, aby odhalila nejen známé hrozby, ale také anomálie uživatelského chování. Chceme mít tak dobrá bezpečnostní opatření, aby přímo konkurovala moderním hrozbám.

Technologie se budou měnit, lidská povaha zůstane stejná. Navzdory rychlému technologickému vývoji zůstávají základní principy útoků stejné: manipulace, důvěra a lidská chyba. Budoucnost kybernetické bezpečnosti tak zůstane především otázkou lidských rozhodnutí.

Závěr

Celá kniha byla věnována paradoxům ze světa kybernetické bezpečnosti. Snažil jsem se čtenáři přiblížit vlastní pohled na paradoxy týkající se témat, se kterými se běžně setkávám. Nejsou zde obsaženy všechny existující paradoxy, to z podstaty tématu ani není možné. Mým hlavním úmyslem je inspirovat ostatní k cílenému a užitečnému zpochybňování. Ničemu se nedá plně důvěřovat. Vždy existuje vícero cest pro dosažení cíle. Musíme hledat alternativy, rizika a možnosti.

Nejzásadnější myšlenku jsem si záměrně nechal na úplný závěr. A ta zní, že i paradox samotný může být paradoxem. Z mého pohledu tento jev nastává, když naše snaha paradox vyřešit ho zároveň vytváří, posiluje nebo rozvíjí. Kybernetická bezpečnost je proces s cílem odstranění nejistoty z prostředí, které je nejistotou definováno. Čím lépe systém vytvoříme, tím více spoléháme na to, že je bezpečný. Spoléhání se na stabilitu a bezpečnost systému vytváří nové zranitelnosti. Například slepotu vůči selhání. Neschopnost řešit

problém, který jsme nikdy neočekávali a nevyhodnocovali.

Každé další bezpečnostní opatření má za úkol nám pomoci chránit se před kybernetickým útokem. Zároveň nás však pouhé hromadění nástrojů může připravit o schopnost uvěřit, že kybernetický útok právě probíhá.

Bezpečnost na internetu je velmi křehká. Nikdy nejde vyřešit úplně. To nás ovšem nesmí vést k rezignaci. Naopak by nás to mělo vybudit k tomu, abychom nebrali situaci na lehkou váhu. Největším paradoxem kybernetické bezpečnosti není to, že nikdy není úplná. Největším paradoxem je, že pochopení této neúplnosti nás může učinit buď ostražitějšími, nebo lhostejnějšími. Možná největší hrozbou není to, co jsme ještě nezabezpečili, ale to, čemu jsme už začali bezvýhradně věřit.

Tato kniha nemá být seznamem odpovědí. Má být spíše připomínkou, že dobré bezpečnostní rozhodnutí často začíná nepříjemnou otázkou. Kde končí ochrana a kde začíná falešný pocit bezpečí?

O autorovi

Marek Kovalčík je odborníkem v oblasti kybernetické bezpečnosti, hackování a penetračního testování. Podílel a podílí se na zakázkách pro klienty ze soukromého sektoru i pro veřejné subjekty různých velikostí, jak v České republice, tak i v zahraničí. Po absolvování studia informačních technologií na Vysokém učení technickém v Brně rozšířil své znalosti studiem risk managementu na Ústavu soudního inženýrství, čímž získal komplexní pohled na technologické a právní aspekty digitální sféry.

Ve svých kariérních začátcích se věnoval programování, ale brzy ho zlákaly oblasti s širším záběrem, jako jsou operační a informační systémy, počítačové sítě a komunikace, se zvláštním důrazem na jejich bezpečnostní aspekty.

Marek je držitelem několika prestižních certifikací, včetně CISSP, C|CISO, C|OSINT, CEH, ISTQB, což dokládá jeho odbornost a závazek k budování bezpečnosti informačních systémů.

Tato kniha by nevznikla v podobě, v jaké ji právě držíte v rukou, bez podpory a cenných podnětů mnoha lidí. Mé upřímné poděkování patří všem, kteří se podíleli na jejím vzniku, ať už svými odbornými připomínkami, pečlivou jazykovou a stylistickou korekturou, kritickým pohledem na obsah, nebo ochotou věnovat svůj čas otevřeným diskusím nad jednotlivými kapitolami. Každá připomínka, otázka i odlišný pohled pomohly tuto knihu posunout o krok dál.

Děkuji

Vydal Marek Kovalčík
Brno, 2026

PARADOXY KYBERSVĚTA

aneb bezpečnost v nejistotě

Když se řekne „kybernetická bezpečnost“, mnoho z nás si představí antiviry, firewally a složité technologie, které mají chránit naše systémy před útočníky. Firmy investují miliony do ochrany své infrastruktury, budují bezpečnostní týmy a zavádějí přísná pravidla. Čím více však moderní organizace spoléhají na technologie, tím více se jejich fungování stává závislé na systémech, které samy o sobě nejsou dokonalé. Digitální svět je plný rozporů. Technologie, které mají organizace chránit, je mohou zároveň oslabovat. Kybernetické hrozby dnes nejsou jen technickým problémem – jsou strategickou výzvou, která ovlivňuje způsob, jakým moderní organizace fungují a rozhodují se.