cyllium

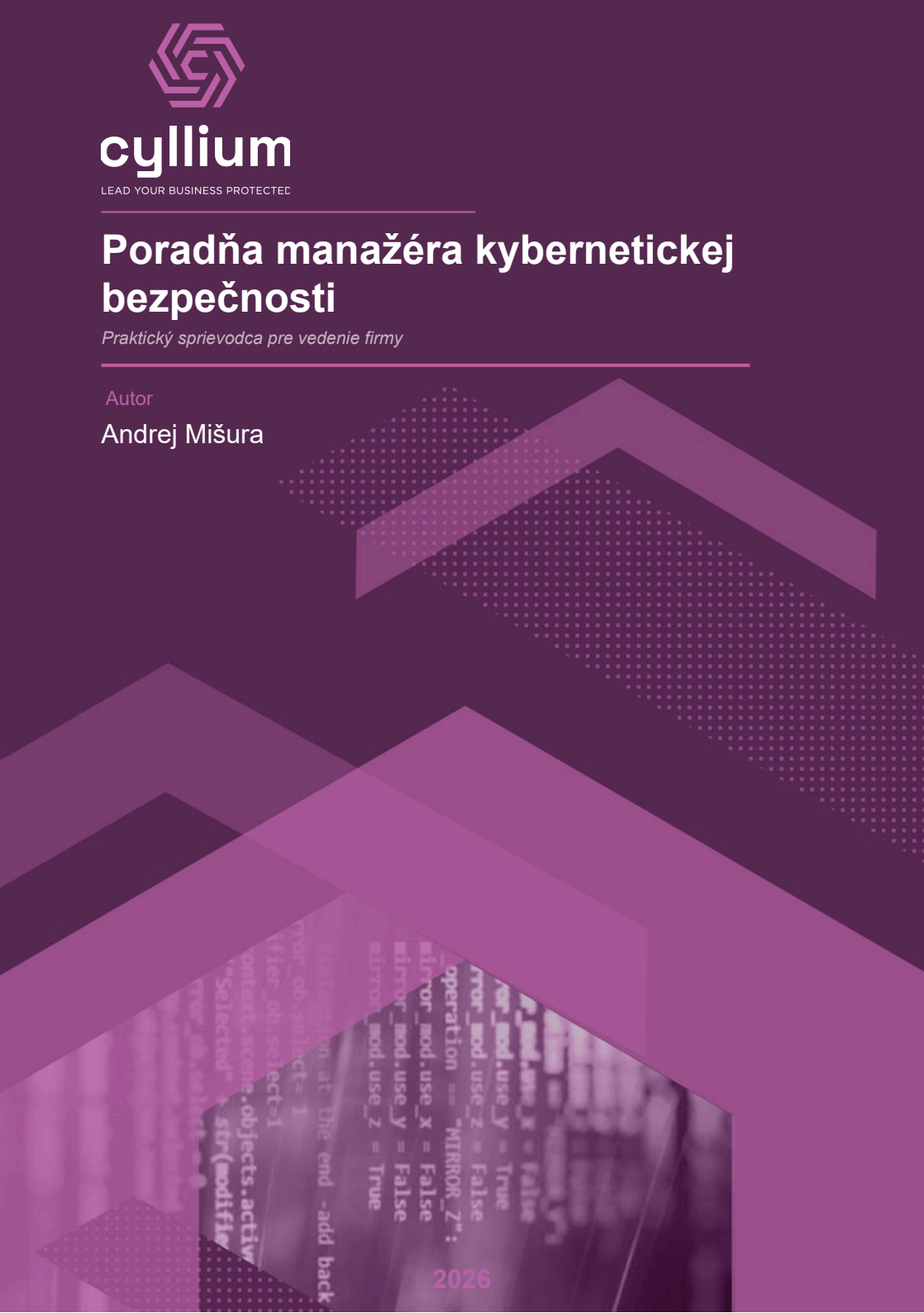
LEAD YOUR BUSINESS PROTECTED

Poradňa manažéra kybernetickej bezpečnosti

Praktický sprievodca pre vedenie firmy

Autor

Andrej Mišura



2026

Dvanásť mesiacov, jeden cieľ: ochrániť to, čo ste vybudovali

Kybernetická bezpečnosť dnes nie je témou výlučne pre IT oddelenie. Je to manažérska disciplína, ktorá sa týka výroby, obchodu, logistiky, financií aj ľudí.
Poradňa manažéra kybernetickej bezpečnosti prináša modelový príbeh ročnej spolupráce vedenia firmy a manažéra kybernetickej bezpečnosti. Ukazuje, ako systematicky budovať ochranu firmy bez chaosu, bez zbytočnej byrokracie a bez paralýzy bežného fungovania.

Na ilustráciu sme vytvorili fiktívnu firmu, výrobcu proteínových tyčiniek a špeciálnej výživy – typická slovenská firma, na ktorú sa vzťahujú povinnosti podľa zákona o kybernetickej bezpečnosti.

Do slovenských firiem dnes nastupujú stovky manažérov kybernetickej bezpečnosti. Manažment, špecialisti, zamestnanci aj dodávatelia sa učia spolupracovať v novej digitálnej realite — a nie vždy vedia ako.

Každý mesiac riešime jednu kľúčovú oblasť.
Cestu od nástupu manažéra kybernetickej bezpečnosti do práce môžete absolvovať v mesačných etapách, alebo si takto porovnať svoje postupy a plány. Spolu tvoria ucelený rámec, ktorý môžete aplikovať vo vlastnej firme.

Ako čítať túto poradňu?

- Ako praktický manuál krok za krokom.
- Ako inšpiráciu pre vlastnú firmu.
- Ako kontrolný zoznam pre porovnanie vlastného stavu.
- Ako strategický rámec pre plánovanie nasledujúceho roka.

„Riziko je prirodzenou súčasťou podnikania. Skutočnou výzvou však je, či ho vieme riadiť.“

Obsah

01 **Rozumiete vlastnej firme dostatočne na to, aby ste ju vedeli ochrániť?**
Spoznávame procesy, vzťahy, kritické miesta. Vytvárame plán. Získavame podporu vedenia.

02 **Viete, v akom stave je vaša bezpečnosť dnes?**
Robíme vstupný audit. Bez ilúzií. Bez ružových okuliarov. Overujeme zákonné povinnosti.

03 **Viete presne, čo má vo vašej firme najvyššiu hodnotu?**
Mapujeme aktíva, ich vlastníkov a závislosti. Zavádzame klasifikáciu informácií.

04 **Čo by sa stalo, keby zajtra vypadol váš kľúčový systém?**
Analyzujeme dopady. Vyhodnocujeme riziká. Nastavujeme priority ochrany.

05 **Máte bezpečnosť pod kontrolou, alebo len definovanú v dokumente?**
Formalizujeme riadenie. Nastavujeme merateľné ciele. Zavádzame kontrolný systém.

06 **Je vaša infraštruktúra skutočne chránená?**
Implementujeme technické opatrenia. Segmentácia. Riadenie prístupov. Monitoring. Zálohy.

07 **Prežije váš biznis výpadok?**
Pripravujeme plán kontinuity. Testujeme obnovu. Simulujeme krízové situácie.

08 **Viete, kto robí čo, keď sa niečo pokazí?**
Nastavujeme proces riešenia incidentov. Jasná eskalácia. Jasná zodpovednosť.

09 **Sú vaši ľudia prvou líniou obrany, alebo najväčším rizikom?**
Školíme zamestnancov. Testujeme pripravenosť. Upravujeme zmluvy s dodávateľmi.

10 **Ak stojí výroba, stojí firma. Chránite výrobu?**
Zabezpečujeme OT prostredie, výrobnú infraštruktúru a riadiace systémy.

11 **Ste pripravení pozrieť sa do zrkadla?**
Interný pred-audit. Systematická príprava na externé overenie.

12 **Čo sa podarilo a kam idete ďalej?**
Vyhodnocujeme rok. Upravujeme stratégiu. Nastavujeme vyššiu úroveň zrelosti.

O autorovi

Andrej Mišura je CEO skupiny Cyllium, certifikovaný audítor a manažér kybernetickej bezpečnosti s viac ako dvadsiatimi rokmi skúseností.

V roku 2024 bol vyhlásený za CISO of the Year.

Je držiteľom certifikátov CISA, CISM, CDPSE, CEH, MCSE a je expertom na štandard ISA 62443.

Túto poradňu som napísal s cieľom poskytnúť organizáciám jasný a praktický rámec, ktorý im pomôže zorientovať sa v kybernetickej bezpečnosti, pochopiť kde začať a na čo sa zamerať ako prvé, aby ju mohli systematicky budovať a riadiť.

Rozumiete vlastnej firme dostatočne na to, aby ste ju vedeli ochrániť?

Som manažérom kybernetickej bezpečnosti. Moja úloha je jasná – zabezpečiť, aby všetko od receptov až po zákaznícke dáta zostalo chránené a proces výroby a distribúcie bežal bez problémov.
Na prvý pohľad to znie jednoducho, no veľmi rýchlo som pochopil, že pred sebou mám veľkú výzvu. V praxi ide o zásah do fungovania celej organizácie.

Získavanie spojencov

Prvé dni som neotváral technické manuály. Chodil som po firme. Prešiel som výrobnú halu. Rozprával som sa s majstrami, IT administrátormi, účtovníkmi aj obchodníkmi. Pýtal som sa rovnaké otázky: Čo je pre vás kritické? Čo by vás okamžite zastavilo? Kde vidíte najväčšie riziko?
Ich odpovede mi dali cennejšie informácie než akýkoľvek auditný checklist. Ukázali mi, kde firma skutočne žije a kde je zraniteľná.

Diskusia s vedením

Bez podpory vedenia sa bezpečnosť stáva iba odporúčaním. S podporou vedenia sa stáva prioritou.

Hneď na začiatku som išiel za generálnym riaditeľom. Vedel som, že ak nezískam jeho podporu, skončil som. Vysvetlil som mu, že ako štatutár nesie zodpovednosť za ochranu údajov aj za kontinuitu výroby. A keďže sme aj PZS – prevádzkovateľ základnej služby, tak táto zodpovednosť má dokonca trestnoprávny rozmer.
Na stretnutie som priniesol konkrétny plán činností na rok a ukázal som mu, že bezpečnosť nie je len náklad, ale investícia, ktorá môže zachrániť firmu pred katastrofou. Máme predsa spoločný cieľ - aby firma vyrábala aj zajtra. Po chvíľke ticha mi podal ruku a povedal: „Andrej, máš moju podporu. Ideme na to."

Nastavenie očakávaní

S vedením sme si zadefinovali, čo bezpečnosť nie je – nie je to jednorazový projekt, nie je to len IT záležitosť a nie je to niečo, čo sa urobí raz a je hotové. Bezpečnosť je kontinuálny proces, ktorý si vyžaduje ľudí, čas a premyslené rozhodnutia.

Bezpečnostný výbor

Je snáď samozrejmosťou, že bez zapojenia manažmentu sa nič nepohne. Ako prvý krok som na porade vedenia navrhol založenie bezpečnostného výboru, čo je vlastne tím na prijímanie strategických rozhodnutí v oblasti kybernetickej bezpečnosti. Tím som poskladal z ľudí, ktorí vedia, ako firma žije – od IT cez výrobu, HR až po financie. Generálny riaditeľ prijal rolu predsedu výboru.
Výbor bude našou platformou na diskusiu o rizikách, návrhoch riešení a rozhodnutiach. Stretávať sa budeme pravidelne každý mesiac a vždy vyhodnotíme, čo sa podarilo a kde máme rezervy.

Plán namiesto improvizácie

Na prvom stretnutí výboru som im predstavil konkrétny ročný plán-harmonogram aktivít na každý mesiac. Nie všeobecné frázy, ale jasné kroky, termíny a očakávané výstupy.

Skutočný začiatok

Budovanie bezpečnosti nie je o komplikovaných technológiách. Je o správne položených základoch:

- pochopení biznisu,
- jasne definovaných zodpovednostiach,
- podpore vedenia,
- postupnosti krokov.

Ak vedenie chápe význam bezpečnosti, tento postoj sa prirodzene prenesie aj na zamestnancov. A práve tam začína skutočná zmena kultúry.

Poznámky

Viete, v akom stave je vaša bezpečnosť dnes?

Po prvom mesiaci už rozumiem tomu, ako firma funguje, ktoré procesy sú kritické a kde sa nachádzajú citlivé miesta. Intuícia však nestačí. Bezpečnosť sa nedá riadiť pocitmi. Potrebujeme fakty.
Zistili sme, že naša modelová firma spĺňa identifikačné kritériá podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. Je prevádzkovateľom základnej služby – to znamená vyššiu mieru zodpovednosti aj povinností.
Skutočný obraz úrovne bezpečnosti poskytne iba systematické technologické a procesné overenie. Až to odhalí silné stránky aj slabiny našej ochrany.

Bezpečnostná „zdravotná prehliadka"

Overenie stavu bezpečnosti možno prirovnať k preventívnej prehliadke. Nejde o hľadanie vinníkov. Ide o stanovenie východiskovej pozície – reálne zistiť, kde máme slabé miesta a ako ich odstrániť skôr, než spôsobia vážne škody. Overovanie je rozdelené do troch kľúčových oblastí.

1. GAP analýza – kde máme medzery

Porovnali sme aktuálny stav firemnej bezpečnosti s požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, vyhlášky č. 227/2025 Z. z. o bezpečnostných opatreniach a osvedčenými medzinárodnými štandardmi, napríklad ISO 27001. Identifikovali sme oblasti, kde chýbajú procesy, dokumentácia alebo technologické riešenia v kybernetickej bezpečnosti a kde sú nejasne definované zodpovednosti.
Výsledkom bol zoznam konkrétnych zistení, ktorý sa stal základom priorít pre ďalšie mesiace.

2. Technologické overenie úrovne bezpečnosti – ako sú na tom naše systémy

Technologické overenie úrovne bezpečnosti sa zameriava na posúdenie aktuálneho stavu systémov a infraštruktúry organizácie. V rámci testovania zraniteľností bol použitý špecializovaný nástroj na skenovanie serverov, sieťových zariadení a koncových staníc s cieľom identifikovať kritické bezpečnostné slabiny. Analýza zároveň ukázala, či sú systémy pravidelne aktualizované a či neobsahujú známe zraniteľnosti

Kontrola sa zamerala najmä na základné bezpečnostné opatrenia, ako sú politika hesiel, deaktivácia nepoužívaných služieb a bezpečné nastavenie vzdialeného prístupu. Samostatná pozornosť bola venovaná prostrediu Microsoft Active Directory Domain Services, ktoré predstavuje kľúčový prvok riadenia prístupov v organizácii. Overenie sa zároveň rozšírilo aj na cloudovú infraštruktúru Microsoft 365, kde sme cez Secure Score skontrolovali viacfaktorovú autentifikáciu a nastavenia zdieľania citlivých dokumentov.

3. Procesné overenie – ako je bezpečnosť riadená

Procesné overenie sa zameralo na spôsob riadenia bezpečnosti v organizácii, keďže samotná technológia predstavuje iba časť celkového obrazu. Posudzovali sme proces riadenia zmien v IT infraštruktúre, ktorý má zabezpečiť, aby boli všetky zmeny v konfiguráciách, serveroch, sieťach alebo aplikáciách riadne schválené, evidované a otestované.
Súčasťou hodnotenia bol manažment záplat – pravidelný mechanizmus na kontrolu a nasadzovanie bezpečnostných aktualizácií. Overili sme procesy zálohovania a kontinuity prevádzky, vrátane frekvencie záloh a testovania obnovy.

Výsledky sú na stole

Výsledky hĺbkového overenia úrovne bezpečnosti som predstavil bezpečnostnému výboru. Niekedy to nie je príjemné počúvanie, no vedenie prijalo fakty. Zložili sme si ružové okuliare.

Overenie nebolo len papierovou byrokraciou. Bol to prvý skutočný pohľad do bezpečnosti firmy a jasný signál, že je čas konať.

Poznámky

Viete presne, čo má vo vašej firme najvyššiu hodnotu?

Skôr než začneme zavádzať opatrenia, musíme si odpovedať na základnú otázku: Čo vlastne chránime? Bez tejto odpovede nie je možné budovať bezpečnostnú stratégiu.

Čo sú to aktíva?

Aktívum je všetko, čo má pre firmu hodnotu. Rozdelili sme ich do piatich kategórií: informačné aktíva (zmluvy, databázy, receptúry), fyzické aktíva (servery, výrobné linky), softvérové aktíva (ERP, skladový softvér), služby (internet, cloud, partneri) a ľudské zdroje (know-how, prístupové oprávnenia).

Každé aktívum má svojho vlastníka

Ku každému aktívu sme priradili konkrétneho vlastníka – nie IT oddelenie ako celok, ale konkrétnu osobu. Vlastník musí vedieť, na čo aktívum slúži, aký je jeho význam pre firmu a kto má reagovať pri incidente.

Bez vlastníctva neexistuje zodpovednosť.

Klasifikácia: čo je skutočne kritické

Každé aktívum sme s vlastníkmi posúdili z pohľadu troch vlastností: integrita, dostupnosť a dôvernosť. Zároveň sme aktívum a jeho vlastnosti klasifikovali podľa dôležitosti a vplyvu na chod firmy.

Inventár ako živý dokument

Výsledkom inventarizácie nie je statická tabuľka. Je to živý register, ktorý odráža aktuálny stav firmy. Každá zmena – nový systém, nový zamestnanec, nový dodávateľ – sa musí prejaviť aj v inventári. Preto sme zaviedli pravidelný štvrťročný prehľad, kde vlastníci potvrdzujú aktuálnosť svojich aktív.

Čo nás prekvapilo

Počas inventarizácie sme narazili na systémy, o ktorých IT oddelenie ani nevedelo. Starší výrobný softvér bežal na stroji bez záplat. Zálohy jedného kritického systému smerovali na rovnaký server, ktorý zálohujú – čo v prípade výpadku servera znamená stratu oboch kópií. Tieto zistenia by pri útoku mohli byť fatálne.

Aktíva nie sú izolované

Aktíva nefungujú samostatne. Fungujú v prepojených systémoch. Receptúra je uložená na serveri, server beží v sieti, prístup je riadený centrálnym systémom. ERP systém prepája objednávky, sklad aj výrobu. Výpadok jedného prvku môže narušiť celý reťazec.
Preto sme si do inventára zaznačili aj väzby a nadväznosti medzi aktívami, čiže kto sa na koho „spolieha“. Práve tento pohľad je základom pre analýzu dopadov (BIA).

Červené zóny

Na základe hodnotenia dopadu a závislostí sme identifikovali kritické aktíva, tzv. červené zóny: ***zdieľaný sieťový prvok***, cez ktorý komunikuje ekonomický systém, výroba aj zálohy, ***výrobný systém***, bez ktorého nie je možné vyrábať, ***ERP systém***, ktorý riadi fakturáciu, objednávky, sklad a napojenie na výrobu.
Tie sme zaradili medzi najvyššie priority na ďalšie zabezpečenie.

Životný cyklus aktív

Inventarizácia nebola len jednorazová úloha. Bola to dôkladná príprava na ďalší krok: Business Impact Analysis. Tá nám pomôže zistiť, čo sa stane, keď niektoré aktívum zlyhá? Koľko času si môžeme dovoliť byť bez ERP? Čo spôsobí výpadok výrobného systému? Ako rýchlo potrebujeme obnoviť prístup k zálohám?

Dnes vieme čo máme, kto za to zodpovedá, akú to má hodnotu a ako sú aktíva navzájom prepojené. Tento základ nám umožní zavádzať opatrenia, ktoré budú dávať zmysel v praxi.

Poznámky

Čo by sa stalo, keby zajtra vypadol váš kľúčový systém?

Výsledkom inventarizácie a klasifikácie aktív je prehľad o tom, čo máme, čo je dôležité a kto za čo zodpovedá. Čo sa ale stane, ak niektoré z týchto aktív alebo služieb zlyhajú?

Na túto otázku nám odpovedajú dva nástroje ***analýza dopadov (BIA) a analýza rizík.***

Analýza dopadov (BIA)

Spolu s vlastníkmi procesov sme si položili jednoduchú otázku: Ak konkrétny systém vypadne, aký bude dopad na firmu?
Z tejto diskusie vznikli dva kľúčové parametre:

- RTO (Recovery Time Objective) – maximálny čas, do ktorého musí byť služba obnovená, aby firma neutrpela vážnu škodu;
- RPO (Recovery Point Objective) – maximálny objem dát, ktoré si môžeme dovoliť stratiť.

__ERP systém:__ obnova do 8 hodín, prípustná strata dát max. 4 hodiny.
__Výrobný softvér:__ obnova do 4 hodín, prípustná strata iba 1 hodina.
Tieto čísla nie sú technické parametre – sú to obchodné rozhodnutia.

Mapa závislostí

Nestačí obnoviť jeden systém. Musíme obnoviť celý funkčný reťazec.
Preto sme vytvorili mapu závislostí medzi procesmi a aktívami.
Z nej vyplýva poradie obnovy. Vieme, čo musí byť dostupné ako prvé, aby sa zvyšok mohol spustiť.Práve tu sa ukazuje význam investícií do infraštruktúry, ktorá je bežne „neviditeľná“.

Analýza rizík

Keď vieme, aký je dopad výpadku, ďalšou otázkou je: **Čo môže taký výpadok spôsobiť?**
Riziko sme hodnotili ako kombináciu pravdepodobnosti a dopadu.
Vytvorili sme konkrétne scenáre:

- Výpadok ERP počas expedície – faktúry neodídu, objednávky sa zaseknú.
- Ransomvér cez podvodný e-mail – výpadok viacerých oddelení naraz.
- Výpadok sieťového prvku vo výrobe – škoda na materiáli a reputácii.

Ošetrenie rizika v praxi

Kybernetická bezpečnosť funguje na princípe viacerých vrstiev ochrany, nie jedného opatrenia. Napríklad riziko ransomvéru sa výrazne znižuje kombináciou offline záloh, školenia zamestnancov a e-mailového filtrovania. Každá vrstva zachytí časť hrozby, ktorú by samostatné opatrenie nemuselo odhaliť. Aj preto sa bezpečnosť vždy buduje ako systém, nie ako jedno riešenie.

Prepojenie rizík a opatrení

Scenáre sme spojili s existujúcimi opatreniami a zistili sme, kde máme rezervy a navrhli bezpečnostné opatrenia. Technické zmeny môžu byť monitoring, zálohy, alebo segmentácia. Logovanie, schvaľovanie a obnova sú procesné kroky a medzi organizačné opatrenia patria zodpovednosti, školenia a testovanie.

Čo tým získavame?

Analýza dopadov a rizík nie je formálne cvičenie pre audítora. Je to rozhodovací nástroj pre vedenie firmy.Pomohli nám odpovedať na otázky:

- Čo sa nám môže stať?
- Ako rýchlo musíme reagovať?
- Koľko nás bude stáť, ak to zanedbáme?

Bezpečnosť už neriešime ako izolovaný IT problém, ale ako firemnú zodpovednosť. Každý proces má svoj dopad a každé riziko má svojho vlastníka.

Poznámky

Máte bezpečnosť pod kontrolou, alebo len v dokumente?

Doteraz sme zbierali informácie, analyzovali dopady a riziká, pomenovali kritické aktíva a nastavili si priority. Teraz prichádza ďalší krok – dokumentácia, smernice a systémové riadenie.

Bez systému sa bezpečnosť stáva reakciou na incidenty. So systémom sa stáva riadeným procesom.

Začíname formálne riadiť bezpečnosť

Formalizácia neznamená byrokraciu. Znamená jasnosť. Každý musí vedieť:

- čo má robiť,
- prečo to robí,
- ako sa vyhodnotí, že to funguje.

Cieľom nie je naplniť paragrafy. Cieľom je zabezpečiť, aby ochrana firmy fungovala aj o rok.

Bezpečnostná politika sú základné pravidlá hry

Je to základný dokument, ktorému má rozumieť vedenie aj zamestnanci. Definuje, čo pre nás znamená bezpečnosť, aké princípy uplatňujeme, aké sú naše zákonné a sektorové povinnosti a čo očakávame od zamestnancov a dodávateľov.
Nie je to technický dokument – je to rámec rozhodovania.

Smernice a postupy

Ak politika definuje smer, smernice určujú spôsob. Zaviedli sme pravidlá pre: riadenie prístupov, klasifikáciu informácií, zálohovanie a obnovu, hlásenie incidentov, riadenie záplat a nástup a výstup zamestnancov.
Každý dokument vznikal v spolupráci s ľuďmi z praxe. Nie ako univerzálna šablóna, ale ako funkčný nástroj prispôsobený realite firmy.
Dokumenty musia byť použiteľné. Inak nemajú hodnotu.

Merateľné ciele - bezpečnosť sa musí dať riadiť

Vyhlásenie „zlepšíme bezpečnosť“ nestačí. Ak má byť bezpečnosť riadená, musí byť merateľná.
Preto sme nastavili konkrétne ukazovatele:

- počet identifikovaných a vyriešených incidentov,

- čas odobratia prístupov pri odchode zamestnanca,
- percento zamestnancov absolvujúcich školenie
- reálny čas obnovy systémov pri testoch,
- čas nasadenia kritických záplat

Nestavali sme ich na ambícii dosiahnuť dokonalosť. Postavili sme ich na reálnych dátach, ktoré sa dajú získať, vyhodnotiť a použiť pri rozhodovaní. Tieto metriky sledujeme každý mesiac na bezpečnostnom výbore. Dávajú nám spätnú väzbu, či kroky, ktoré robíme, prinášajú výsledky. Ak nie, vieme reagovať.

Systém kontrol v praxi

Aby naše ciele neostali len v tabuľke, nastavili sme jednoduchý systém kontrol, ktorý nám dáva pravidelnú a praktickú spätnú väzbu.

- Prístupy sledujeme cez personálne zmeny a overujeme s výstupy zo systému riadenia identít.
- Školenia vyhodnocujeme cez výsledky testu na konci každého školenia.
- Incidenty evidujeme a mesačne vyhodnocujeme ich riešenie a reakčné časy.
- Zálohovanie pravidelne testujeme obnovou vybraných systémov.
- Nasadenie záplat overujeme retestom zraniteľností.

Tieto kontroly sú súčasťou bežného fungovania. Slúžia ako základná spätná väzba pre manažment a zároveň podporujú prípravu na interné audity. Všetky zistenia si evidujeme a používame pri pravidelnom hodnotení stavu bezpečnosti.

Poznámky

Je vaša infraštruktúra skutočne chránená?

Máme za sebou analýzu aktív, klasifikáciu, analýzu dopadov a formalizáciu systému bezpečnosti. Prišiel čas zavádzať konkrétne technické opatrenia podľa Zákona o kybernetickej bezpečnosti.

Zamerali na tieto technické oblasti:

Správa identít a prístupov

Nasadili sme službu Active Directory pre centrálnu správu identít. Zaviedli sme princíp „least privilege“, teda prístup iba k nevyhnutným informáciám. Prístupové práva sme dôsledne prehodnotili, nastavili sme pravidelné kontroly ich aktuálnosti a správnosti, nasadili sme komplexné automatické politiky hesiel.

Systémová, Sieťová a komunikačná bezpečnosť

Implementovali sme firewall s pokročilými funkciami ako IDS, IPS a SSL inspection s hĺbkovou analýzou prevádzky. Efektívna segmentácia siete, kde je výrobná infraštruktúra bezpečne oddelená od administratívnej časti a externých prístupov je už samozrejmosť.

Bezpečnosť koncových zariadení

Nasadili sme komplexné riešenie typu XDR (Extended Detection and Response), ktoré zabezpečuje analýzu a detekciu hrozieb. Prípadná rýchla reakcia na incidenty je už jednoduchšia.

Ochrana e-mailu a webu

E-mail zostáva najčastejšou bránou pre útočníkov. Nasadili sme pokročilý e-mailový filter s antiphishingovými pravidlami, karanténou pre podozrivé prílohy a ochranou pred spoofingom. Na webovú filtráciu sme nasadili DNS-layer bezpečnosť, ktorá blokuje prístupy na škodlivé domény ešte pred načítaním stránky.

Správa zraniteľností a patch management

Systematický proces identifikácie a riadenia reakcie na zraniteľnosti prostredníctvom pravidelných aktualizácií softvéru, operačných systémov a ostatných prvkov infraštruktúry zabezpečujeme centrálny nástrojom na týždennej báze. Patch management je automatizovaný a kontrolovaný, testujeme nasadenie aktualizácií pred ich nasadením do produkcie.

Monitorovanie a riadenie udalostí a incidentov

Všetky kľúčové komponenty infraštruktúry, najmä servery, pracovné stanice, firewall, e mailové brány, VPN prístupy a cloudové služby, posielajú logy do centralizovaného monitorovacieho systému, ktorý ich analyzuje. Bezpečnostné udalosti sú tak viditeľné takmer okamžite a systém umožňuje rýchlu reakciu na podozrivú aktivitu.

Šifrovanie a ochrana dát

Citlivé dáta sú šifrované tak pri prenose, ako aj pri uložení. Zamestnanci pracujúci na diaľku pristupujú k interným systémom výlučne cez VPN s viacfaktorovým overením. Cloudové úložiská prešli bezpečnostnou konfiguráciou – vypnuté verejné zdieľanie, auditné logy aktivované. Tieto opatrenia znižujú riziko neoprávneného prístupu a umožňujú spätne dohľadať každú prácu s dátami.

Zálohovanie a obnova dát

Pravidelne zálohujeme kritické dáta a systémy podľa definovaných RTO a RPO. Zálohy sú bezpečne uložené a testujeme obnovu dát tak, sme zaistili schopnosť rýchleho obnovenia prevádzky v prípade incidentu alebo havárie.

Bezpečnostné opatrenia pravidelne aktualizujeme

Každé technické opatrenie je priamo naviazané na analýzu rizík a predošlé kroky, ktoré sme vykonali.

Naším cieľom nie je len formálny súlad so zákonom, ale skutočná ochrana biznisu.

Poznámky

Prežije váš biznis výpadok?

Technické opatrenia máme nastavené. Teraz sa musíme pripraviť na moment, keď napriek všetkému niečo zlyhá.

Tomu hovoríme plánovanie kontinuity činností. Niektorí to poznajú ako havarijné scenáre. V skutočnosti ide o schopnosť firmy fungovať aj v krízovej situácii.

Bezpečnosť nie je len o tom, ako útoku zabrániť. Je aj o tom, ako pokračovať, keď sa mu zabrániť nepodarí.

Prečo je biznis kontinuita kľúčová?

Pretože nestačí konštatovať, že „nastal problém“.

Musíme vedieť:

- čo presne má pokračovať,
- ako rýchlo,
- v akom poradí,
- s akými minimálnymi nárokmi na techniku a ľudí.
-

Kontinuita nie je plán B. Je to plán, ako prežiť plán A, keď sa pokazí.

Od analýzy k praktickému plánu

Vychádzali sme z výsledkov analýzy dopadov. Identifikovali sme kritické procesy – výrobu, expedíciu, objednávky, komunikáciu so zákazníkmi – a k nim sme priradili konkrétne časové limity obnovy.
Znovu sme si potvrdili RTO, teda maximálny čas výpadku, ktorý si ešte vieme dovoliť, a RPO, teda koľko dát môžeme stratiť bez zásadného dopadu.

Procesy sme následne prepojili so systémami, infraštruktúrou a ľuďmi, od ktorých závisia. Ukázalo sa, že aj nenápadné IT služby sú priamo naviazané na výrobu a expedíciu. Obnoviť jeden systém nestačí. Musíme obnoviť celý funkčný reťazec.

Zálohy nestačia, musia fungovať

Teoretická existencia záloh neznamená schopnosť obnovy. Preto sme obnovu zo záloh reálne otestovali v kontrolovanom režime. Obnovili sme vybrané systémy, preverili čas obnovy a porovnali ho s nastaveným RTO.

A áno, pár vecí nás prekvapilo – objavili sa drobné technické závislosti aj nejasnosti v zodpovednostiach, ktoré by sa v krízovej situácii mohli stať kritickými. Zistenia sme zapracovali do plánu.

Simulácia krízy

Nezostali sme však len pri technickom teste. Urobili sme aj simulačné cvičenie – modelový výpadok kľúčového systému. Bez veľkého varovania. Cieľom nebolo hľadať vinníka, ale zistiť, či plán žije.
Zrazu sa objavili otázky, ktoré v dokumente vyzerali jednoducho:

- Kto vyhlasuje krízový režim?
- Kto komunikuje so zákazníkmi?
- Kto rozhoduje o poradí objednávok?

Pravidelné opakovanie takýchto cvičení je rovnako dôležité ako samotné vytvorenie krízového plánu. Organizácia si tým overuje pripravenosť tímu, aktuálnosť kontaktov a funkčnosť nastavených postupov. Krízový plán tak nezostáva len dokumentom, ale stáva sa praktickým nástrojom riadenia mimoriadnych situácií.

Dnes máme jasne definované scenáre, poradie obnovy, kontakty aj rozhodovacie právomoci. Definovali sme aj minimálny režim fungovania – koľko vieme vyrobiť, ako evidujeme objednávky bez systému a ako komunikujeme v obmedzenom režime.

Kríza nie je otázkou «či». Je otázkou «kedy». Rozdiel je len v tom, či nás zastihne pripravených.

Poznámky

Viete, kto robí čo, keď sa niečo pokazí?

Technológie zlyhávajú, ľudia robia chyby a útočníci nespia. Tak sa pripravme.

Nastavujeme systém riešenia kybernetických incidentov. Nie preto, že by sme chceli niekoho strašiť, ale preto, že je to realita. Pamätajte, že incident nie je zlyhanie, je to test pripravenosti. Rozdiel medzi chaosom a zvládnutou situáciou spočíva v tom, či máme jasný postup a vytrénovaný tím.

Incident ako súčasť reality

Hlásenie incidentu nie je priznanie chyby. Je to ochranný mechanizmus firmy. Čím skôr sa o incidente dozvieme, tým rýchlejšie vieme reagovať. Zaviedli sme jednoduchý a dostupný kanál na hlásenie podozrení a definovali sme interné kategórie incidentov – od podozrenia až po potvrdený útok – a jasné pravidlá eskalácie. Každý vie, komu informáciu odovzdať a kedy sa situácia presúva na úroveň krízového tímu.

Riešenie incidentu v štyroch fázach

Ak už príde k najhoršiemu, incident sa rieši v krokoch.

Najskôr identifikujeme, čo sa stalo, kde vznikol problém a kto ho zaznamenal. Následne analyzujeme rozsah a dopad – čo je zasiahnuté, aké sú možné dôsledky pre prevádzku a zákazníkov.
Nasleduje reakcia: izolácia napadnutých systémov, odstránenie príčiny a nápravné opatrenia. Poslednou fázou je obnova prevádzky a poučenie – spätná analýza, úprava opatrení a posilnenie ochrany.

Každý krok má určenú zodpovednú osobu a presný postup. Incident sa dokumentuje, pretože bez záznamu neexistuje poučenie.

Učíme sa z reality

Čo sa týka nás, profesionálov, učíme sa stále. Z vlastných incidentov, ale aj z cudzích a pravidelne sledujeme varovania NBÚ a zahraničné reporty.
Bezpečnosť nie je statická. Je to neustály proces zlepšovania.

Simulácie namiesto improvizácie

Plán na papieri nestačí. Preto pravidelne organizujeme simulované cvičenia – modelový phishing, výpadok systému, reakciu krízového tímu v reálnom čase.
Výsledok? Niektorí zistili, že vedia reagovať lepšie, ako čakali. Iní, že im chýbali informácie. Aj to je zmysel cvičenia. Pripravenosť znamená "chladnú hlavu" v kríze.

Cieľom je odhaliť slabé miesta ešte predtým, ako ich odhalí útočník.

Kultúra, nie strach

Dôležité je uviesť, že incidenty monitorujeme aj technicky prostredníctvom centralizovaného dohľadu. Čím skôr ich zachytíme, tým menší je ich dopad a menej bolia.
Z každého incidentu pripravujeme poučenie pre vedenie – anonymizované, vecné a orientované na zlepšenie. Chceme budovať kultúru otvorenosti, nie strachu.

Incident je otázkou času. Pripravenosť je otázkou rozhodnutia.

Záchrana reputácie

Technické zvládnutie incidentu je len polovica úspechu. Rovnako dôležité je zvládnuť komunikáciu smerom k zákazníkom, partnerom a verejnosti. Preto máme pripravené šablóny správ a komunikačné scenáre pre rôzne typy incidentov. Základné pravidlo je jednoduché: informovať včas, pravdivo a s jasným plánom nápravy.

Poznámky

Sú vaši ľudia prvou líniou obrany, alebo najväčším rizikom?

Som presvedčený, že kybernetická bezpečnosť je najmä o ľuďoch a nastavení pravidiel s dodávateľmi. Najlepšia stratégia je incidentom predchádzať.

Školenia, ktoré dávajú zmysel

Bezpečnostné školenie nesmie byť formálna povinnosť na intranete. Musí byť zrozumiteľné, praktické a zapamätateľné a preto sme ho postavili na reálnych príkladoch, bez technického žargónu, v krátkych dvadsaťminútových blokoch, s presahom do osobného života.
Ukázali sme si, ako vyzerá podvodný e-mail, čo robiť pri podozrení na incident, ako nešíriť paniku a ako nenaletieť.
A aby si to ľudia naozaj zapamätali, urobili sme aj simulovaný phishingový test. Výsledky? Prvé prekvapenia, ale aj zvedavosť a dobré otázky.

Kultúra namiesto jednorazovej aktivity

Bezpečnostné povedomie sa nebuduje jedným školením. Vytvárame si kultúru, kde sa o *kybernetickej bezpečnosti* hovorí prirodzene, nie formálne. Pridali sme pravidelné pripomienky, nástenky a kvízy – nie ako povinnosť, ale ako pripomienku, že každý môže byť prvou aj poslednou líniou obrany.

Rôzne skupiny, rôzny obsah

Nie všetci zamestnanci potrebujú rovnaké školenie. Výroba má iné riziká ako obchod a IT má iné zodpovednosti ako HR. Preto sme pripravili tri verzie školenia: základné pre všetkých zamestnancov, rozšírené pre vedúcich pracovníkov a technické pre IT tím. S našimi IT špecialistami vedieme workshopy na témy bezpečnej správy IT infraštruktúry, s vývojármi diskutujeme pravidlá bezpečného vývoja a v celej firme sa venujeme pravidlám používania umelej inteligencie s dôrazom na bezpečnosť.

Bezpečnosť ako súčasť kultúry

Skutočná zmena nastala vtedy, keď zamestnanci začali sami hlásiť podozrivé e-maily. Prvý mesiac prišli 3 hlásenia. Po šiestich mesiacoch ich bolo 28 mesačne. Bezpečnosť sa prestala vnímať ako IT problém a stala sa vecou každého.

Dodávateľ nie je cudzí, je naša rozšírená firma

Kybernetický incident u dodávateľa môže mať rovnaký dopad ako incident vo vlastnom systéme.

Preto venujeme pozornosť našim externým partnerom a vychádzame z jednoduchého princípu: Náš dodávateľ je naša zodpovednosť.
Nastavili sme hlavné princípy riadenia dodávateľov: vyberáme ich aj na základe analýzy rizík, overujeme ich bezpečnostnú úroveň, zaväzujeme ich zmluvne k ochrane údajov, trváme na možnosti kontrolovať ich úroveň bezpečnostných opatrení aj u ich subdodávateľov.

Zmluva ako bezpečnostný nástroj

Zmluva nie je formalita. Je to nástroj riadenia rizika. Jasne definované pravidlá spolupráce pomáhajú predchádzať nedorozumeniam a zároveň určujú, ako postupovať v prípade bezpečnostného incidentu.
A keď sa niečo pokazí, je dobré mať v nich jasne napísané, čo od koho očakávame.
Prešli sme všetky aktívne zmluvy, určili zodpovedné kontaktné osoby pre incidenty, doplnili a podpísali bezpečnostné doložky. Tie definujú povinnosti pri ochrane dát, oznamovaní incidentov a spolupráci pri riešení bezpečnostných udalostí.
Dodávateľov sme zároveň informovali o našich očakávaniach a bezpečnostných štandardoch. Naším cieľom nie je vytvárať bariéry alebo kontrolný mechanizmus, ale budovať partnerstvá založené na dôvere, transparentnosti a spoločnej zodpovednosti za bezpečnosť.

Ak sa niečo stane, riešime to spolu.

Poznámky

Ak stojí výroba, stojí firma. Chránite výrobu?

Ak linka stojí, firma stojí. Preto sme sa zamerali aj na operačné technológie a zabezpečenie výroby. Ako my hovoríme – na OT.

V našom modeli výroby sme identifikovali desiatky OT komponentov pripojených do siete – riadiace jednotky, dotykové panely, dohľadové systémy, zariadenia na zber dát. Viaceré sú dostupné výrobcom cez internet či technickým správcom a to cez nástroje na vzdialenú správu. A práve tu vzniká riziko.

Výroba je extrémne citlivá na dostupnosť. Každá minúta výpadku znamená finančnú stratu, oneskorené dodávky a reputačné riziko.

Mapovanie OT prostredia

Bezpečnosť OT sa nezačína technológiou. Začína mapovaním. Spolu s tímom výroby sme vytvorili prehľad všetkých zariadení, ich prepojení a prístupov. Každý komponent má svojho vlastníka a jasne definované miesto v sieti.

Segmentácia OT siete

OT časť treba fyzicky oddeliť od zvyšku siete. Kde sa to nedá, treba nasadiť segmentáciu, firewall a monitoring. Všetky kritické spojenia tak prechádzajú kontrolovaným rozhraním. V OT prostredí treba rešpektovať, že sa používajú špecifické komunikačné protokoly a bezpečnostné opatrenia nesmú ohroziť stabilitu výroby.

Monitorovanie OT prevádzky

Zaviedli sme pasívny OT monitoring, ktorý sleduje sieťovú komunikáciu bez aktívneho skenovania zariadení. Každá anomália je zaznamenaná a vyhodnotená.

Fyzická bezpečnosť vo výrobe

Riadiace panely a HMI rozhrania musia byť chránené fyzicky. Zaviedli sme uzamknutie konzoly po nečinnosti, obmedzili USB porty a označili zariadenia, ku ktorým smú pristupovať len autorizované osoby.

Zálohy a obnova konfigurácií

Pri výrobe nejde len o dáta. Ide aj o konfigurácie zariadení. Každé kritické zariadenie má zálohované nastavenia mimo produkčného

prostredia, offline. Kolegovia z výroby vedia, kde zálohy sú, ako sa obnova robí, že všetko musí byť otestované a zdokumentované.

Riadený vzdialený prístup

Dodávatelia majú prístup len cez schválený kanál, v schválenom čase a za prítomnosti nášho človeka. Každé pripojenie sa loguje. Trvalé VPN prístupy pre servis sme zrušili a nahradili prístupmi s časovým obmedzením a dvojfaktorovým overením.

Spoločný jazyk bezpečnosti a výroby

Spolupráca s výrobou je kľúčová. *Kybernetická bezpečnosť* a prevádzka OT si musia vzájomne vysvetliť, čo kto potrebuje. A až potom môže vzniknúť spoločný plán - oni budú aktívni hráči bezpečnosti, my im nebudeme kaziť výrobu. Spoločným cieľom je stabilná a bezpečná prevádzka.

Záplaty v OT prostredí

Zaviedli sme minimálne bezpečnostné požiadavky pre nové OT zariadenia. Každý nový stroj musí spĺňať definované štandardy ešte pred pripojením do siete.

Pravidelne kontrolujeme konfigurácie a pripravili sme si krízové scenáre pre izoláciu výroby od IT časti v prípade incidentu. Operačné technológie už nie sú slepým miestom. Sú súčasťou riadeného bezpečnostného systému.

Vo výrobe je dostupnosť najvyššia hodnota. Bezpečnosť musí túto hodnotu chrániť, nie ohrozovať.

Poznámky

Ste pripravení pozrieť sa do zrkadla?

Máme za sebou takmer rok práce. Zmapovali sme aktíva, urobili sme analýzu rizík, nastavili procesy, zaviedli technické opatrenia aj ochranu výroby. Teraz prichádza téma, ktorá prirodzene vyvoláva napätie – audit kybernetickej bezpečnosti.

Audit nie je hrozba. Je to spätná väzba. Ak nič nenájde, treba spozornieť.

Interný pred-audit

Spravili sme si interný „pred-audit“, taký vlastný pohľad na to, čo reálne funguje.
Skúsili sme obnoviť dáta zo záloh, testovali sme proces riešenia incidentov, overili sme konfigurácie na sieťových prvkoch a preverili sme správnosť pridelených prístupov. Mnohé veci fungovali dobre, niektoré sme ešte doladili.

Audit nie je o papieroch

Audit kybernetickej bezpečnosti nie je o tom, koľko máte dokumentov. Je o tom, či podľa nich konáte. Smernica, ktorú nikto nepoužíva, je len dokument v šuplíku. Skutočná bezpečnosť sa ukazuje v každodenných rozhodnutiach. Tento prístup zdôrazňujem kolegom po celý rok: bezpečnosť nie je formálna povinnosť. Je to výkon.

Audit je tímová záležitosť

Audit sa netýka iba IT. Audit sa týka celej firmy. Zapájame preto výrobu, logistiku, sklad, HR aj manažment. Niekedy sú to práve nenápadné procesy mimo IT, ktoré rozhodnú o tom, či sa incident rozšíri alebo zastaví.

Výroba pripraví postup, čo robiť, ak prestane komunikovať riadiaca jednotka.

HR kontroluje procesy nástupov a odchodov, aby mali prístupové práva vždy aktuálny stav.

Logistika rieši ako pokračovať v expedícii, ak systém nabehne v obmedzenom režime, alebo vôbec. Každý tu má svoju úlohu. Je to tímový šport.

Audit ako príležitosť

Externý audit, ktorý príde po našom internom, odhalí ďalšie slabé miesta. A to je v poriadku. Nie je cieľ dostať jednotku. Cieľ auditu je zistiť, čo ešte vieme zlepšiť, aby naša výroba stála pevne na nohách, aby sme chránili dodávateľov, zákazníkov aj know-how firmy. Je to príležitosť pomenovať veci pravým menom a posúvať sa stále vpred.

Pohľad manažmentu na realitu

Audit zároveň prináša vedeniu firmy jasný obraz o skutočnom stave bezpečnosti. Umožňuje oddeliť pocit bezpečia od reality. Vedenie tak získáva informáciu, či investície do bezpečnostných opatrení prinášajú reálny efekt. Zároveň pomáha určovať priority ďalších investícií a rozhodnutí.

Dôvera zákazníkov a partnerov

Audit má význam aj vo vzťahu k partnerom a zákazníkom. Firma, ktorá vie preukázať, že bezpečnosť pravidelne overuje a zlepšuje, buduje vyššiu dôveru v obchodných vzťahoch. V mnohých odvetviach sa to stáva konkurenčnou výhodou. Partneri tak majú istotu, že spolupracujú s organizáciou, ktorá berie ochranu dát a prevádzky vážne.

Právna a regulačná ochrana

Rovnako dôležitý je aj právny rozmer. V prípade incidentu je audit dôkazom, že firma pristupovala k bezpečnosti zodpovedne a systematicky. To môže zohrávať významnú úlohu pri riešení sporov alebo pri komunikácii s regulátormi. Ukazuje tiež, že organizácia aktívne pracuje na znižovaní rizík a ochrane svojich aktív.

Poznámky

Čo sa podarilo a kam idete ďalej?

Absolvovali sme dvanásť mesiacov manažéra kybernetickej bezpečnosti v bežnej slovenskej firme. Začínali sme od základov. Končíme pri systéme, ktorý má jasné pravidlá, zodpovednosti a merateľné výsledky.

Čo sme dosiahli

Ako *manažér kybernetickej bezpečnosti* som vedel, že to v našej novej firme bude výzva a že budeme musieť konať rýchlo a systematicky. Dnes však vidím, že najdôležitejšie bolo získať si dôveru ľudí okolo seba.

Celý rok bol najmä o spoznávaní. Nielen technológií, ale ľudí a procesov, ktoré držia firmu v chode. Postupne sme zmapovali aktíva, nastavili klasifikáciu, spravili analýzu rizík, zaviedli technické opatrenia, posilnili bezpečnosť prevádzkových technológií, školili zamestnancov a preverili dodávateľov. Každý mesiac priniesol inú tému, no všetky mali spoločný cieľ – systematicky posilniť odolnosť firmy.

Bez skratkovitých riešení. Bez paniky. Bez ilúzie, že existuje rýchle riešenie. Práve trpezlivý a systematický prístup sa ukázal ako najväčšia sila celého procesu. Každý krok, ktorý sme urobili, vytváral pevnejší základ pre ďalší.

Najväčšia lekcia uplynulého roka

Bezpečnosť nestojí na dokumentoch ani technológiách. Stojí na konzistentnosti a každodenných malých rozhodnutiach.

Tieto rozhodnutia nevznikajú na základe príkazov. Vznikajú z pochopenia, prečo má bezpečnosť zmysel. A práve toto pochopenie je najväčším kapitálom každej organizácie.

Najsilnejším momentom roka nebolo zavedenie novej technológie. Najviac ma tešili momenty, keď kolegovia začali konať sami od seba:

- Technik, ktorý odmietol neznáme USB zariadenie.
- HR oddelenie, ktoré navrhlo lepší proces odoberania prístupov.
- Výrobný tím, ktorý otvorene pomenoval slabé miesto ešte predtým, ako sa stalo problémom.

Prečo je užitočné nastaviť si zrkadlo
Rok sme uzavreli interným auditom. Ten nám poskytol objektívny pohľad na to, čo funguje a čo si vyžaduje zlepšenie. Audit pre nás nebol známkou, ale zrkadlom.

A presne o to ide. Napredovať systematicky, bez zbytočnej paniky a bez falošného pocitu, že „už je hotovo“.

Najdôležitejšie však je, že dnes už bezpečnosť nevnímame ako jednorazovú iniciatívu. Stala sa prirodzenou súčasťou riadenia firmy. A práve tento posun je najväčším výsledkom celého roka práce.

Čo nás čaká

Nasledujúci rok už nebude o zavádzaní základov. Bude o zrelosti systému. O menej formálnych postupoch a efektívnych riešeniach, ktoré dávajú zmysel v každodennej praxi. Väčší dôraz budeme klásť aj na ochranu výroby, ktorá je srdcom našej firmy.
Prioritou bude prevencia, včasné odhalenie rizík a schopnosť rýchlo reagovať na incidenty. Rovnako dôležité bude pravidelne preverovať, či opatrenia, ktoré sme zaviedli, stále zodpovedajú realite prevádzky aj vývoju technológií.

Bezpečnosť nie je projekt s dátumom ukončenia. Je to proces, ktorý sa vyvíja spolu s firmou. A práve v tom spočíva jej skutočná hodnota.

Každý nový systém, každá zmena vo výrobe alebo v organizácii, každý nový projekt či investícia prináša nové otázky, na ktoré musí bezpečnostný systém vedieť včas a zodpovedne reagovať.

Poznámky

Skupina CYLLIUM

LEAD YOUR BUSINESS PROTECTED

Kto sme

Skupina CYLLIUM poskytuje komplexné služby v oblasti informačnej a kybernetickej bezpečnosti na Slovensku i v zahraničí. Vykonávame auditné, expertné a technické služby pod dohľadom skúsených profesionálov s medzinárodnými skúsenosťami a certifikáciami. Pomáhame klientom identifikovať hrozby, posúdiť a nastaviť procesy tak, aby dosiahli primeranú úroveň ochrany svojich aktív a zároveň zabezpečiť súlad so štandardmi a legislatívou.

Naše služby

Auditné služby

- Interný a externý audit KB podľa Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti
- Posúdenie riadenia informačnej bezpečnosti podľa štandardu ISO 27001
- GAP analýza/posúdenie súladu podľa Zákona o kybernetickej bezpečnosti
- GAP analýza súladu spracovania osobných údajov s GDPR
- Posúdenie IT prostredia pre účely štatutárneho auditu (ITGC)
- Posúdenie súladu so štandardom PCIDSS, SWIFT, eIDAS, ENSTO-e

Expertné služby

- Návrh bezpečnostných opatrení v organizácii
- Poskytovanie bezpečnostných rolí
- Podpora implementácie bezpečnostných opatrení
- Príprava a aktualizácia bezpečnostnej dokumentácie
- Analýza rizík a dopadov Školenie zamestnancov a dodávateľov
- Riadenie projektu a plánovanie projektových prác

Technologické služby

- Návrh, realizácia, správa a prevádzka:
  - lokálnej infraštruktúry
  - serverovej infraštruktúry
  - virtualizačnej infraštruktúry
  - cloudovej infraštruktúry
  - hybridnej infraštruktúry
  - adresárových služieb a
  - infraštruktúry verejných kľúčov
- Migrácia a konsolidácia prevádzkových infraštruktúr
- Bezpečnostná konfigurácia (Security hardening)
- Zabezpečenie koncových staníc

Naši klienti

Dôverujú nám spoločnosti z rôznych sektorov ekonomiky.

... a ďalší klienti, s ktorými spolupracujeme.

Poznámky

cyllium

LEAD YOUR BUSINESS PROTECTED

info@cyllium.eu
+421 917 553 223
Bottova 2A, Bratislava
www.cyllium.eu

Chránime to, čo ste vybudovali.

auditori.it, s.r.o. | Cyllium SK, s.r.o. | Cyllium IT, s.r.o.