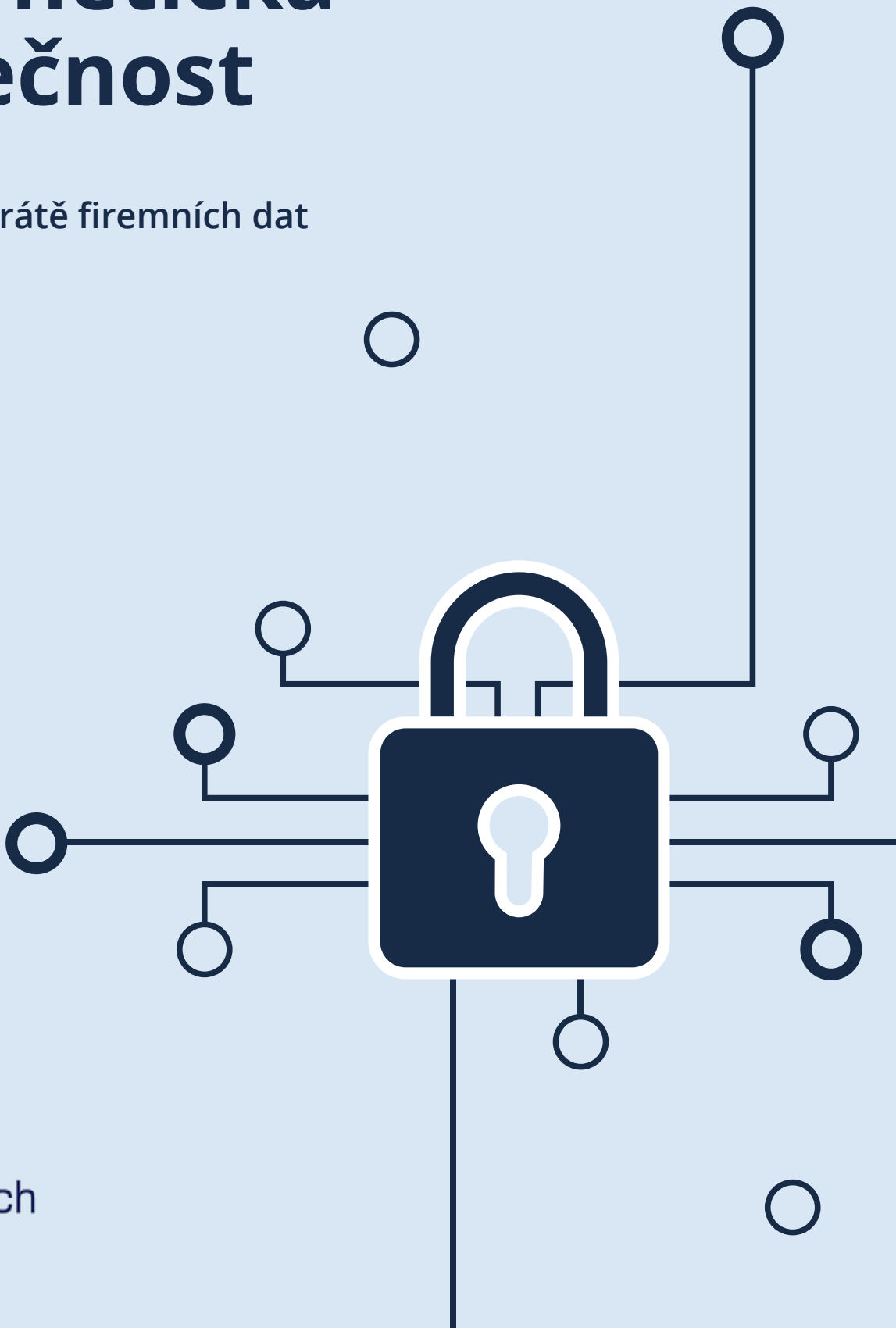
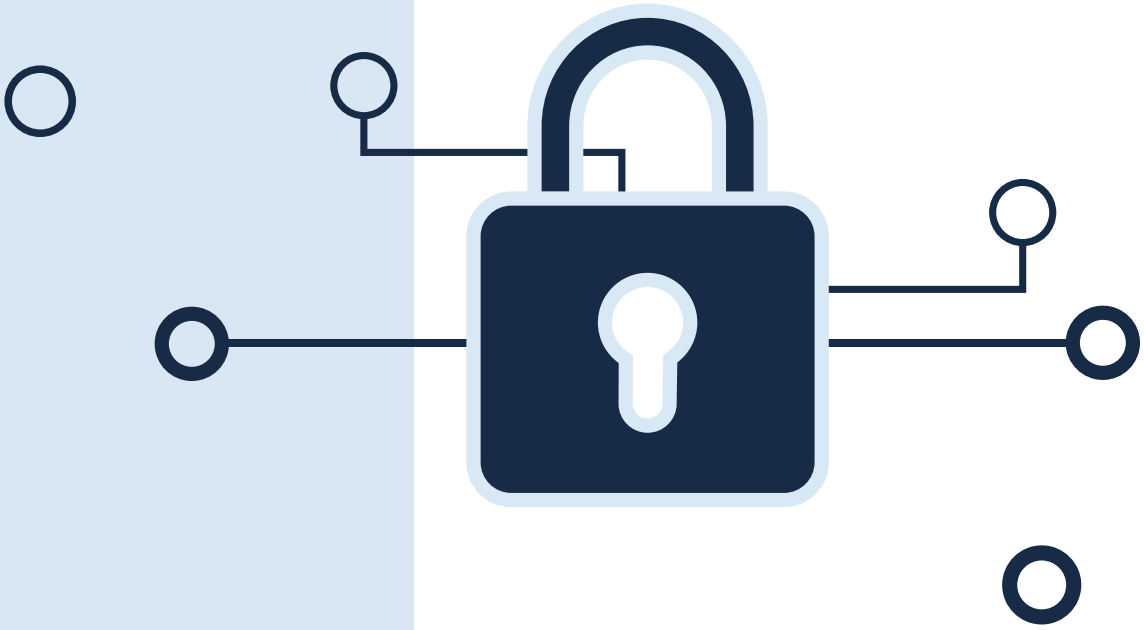
Firemní kybernetická bezpečnost

Jak předejít ztrátě firemních dat



algotech

Obsah



Úvod

Ve světě, který zásadně proměnila digitalizace, automatizace a internet, jsou informační technologie nezbytnou součástí každé firmy. Její výkon je přímo úměrný schopnosti efektivně využívat tyto technologie v rámci běžného fungování, jehož cílem je maximalizace výnosů a zajištění spokojenosti zákazníka. Bez kvalitního IT vybavení by dnes firmy jednoduše nemohly fungovat.

Užívání nejmodernějších technologií, zavádění cloudových řešení a očekávání nepřetržité dostupnosti služeb však klade nesmírně vysoké nároky na správu firemní IT infrastruktury a sítí. To s sebou nese i značnou odpovědnost, protože takto nastavené prostředí je ze své podstaty velmi náchylné k výpadkům či ztrátě dat. A jak odhalily poslední měsíce, IT vybavení firem v České republice není ve většině případů proti kybernetickým hrozbám chráněno dostatečně.

Kybernetické útoky na nemocnice, úřady i soukromé společnosti ukazují, že jediné nezabezpečené zařízení může ohrozit fungování celého podniku. Nejen kvůli ztrátě firemních či zákaznických dat, které dnes tvoří podstatnou část hodnoty každé společnosti, ale také kvůli ohrožení finanční stability napadené firmy. Nedostatečná kybernetická ochrana totiž násobí náklady na bezpečnostní řešení incidentů a kroky vedoucí k omezení jejich dalšího výskytu.

Nemluvě o tom, že ztráta dat a informací má vždy dopad na dobré jméno firem i na důvěru zákazníků, což pro většinu společností znamená ohrožení jejich stávající pozice na trhu nebo dokonce i úplný konec jejich podnikání.

Firemní IT a kybernetickou bezpečnost proto není radno podceňovat. Již dávno totiž neplatí, že „dobrý“ antivirus vyřeší vše. Moderní způsoby útoků jej dokážou snadno obejít a vynutit si často i neuvědomělou aktivitu od samotného uživatele.

Data jsou novodobá ropa

Jejich zabezpečením ochráníte nejen sebe, ale i své zákazníky! Jak toho co nejefektivněji docílit? S pomocí této publikace a odborníků ze společnosti Algotech to může být velmi jednoduché.

IT vybavení firmy

Rozjezd a řízení každé firmy s sebou nesou řadu úkolů, mezi něž zpravidla patří pořízení odpovídajících informačních technologií a výběr příslušných IT služeb. To představuje nejen zajištění hardwarového vybavení zaměstnanců či nalezení nejvhodnějšího softwaru, ale také obstarání serveru a odborníků pro správu, zálohování či zabezpečení všech služeb.

Hardware firmy zpravidla tvoří:

- Servery a datová uložiště
- Mobilní a stolní telefony
- Počítače a notebooky
- Tiskárny a skenery
- Síťové prvky jako například routery, switche apod.
- Další počítačové komponenty

Software firmy zpravidla tvoří:

- **Systémový software a firmware**
  > běžně známý jako operační systém, bez něhož by hardware a jeho části nemohly správně fungovat
- **Aplikační software**
  > především kancelářské a grafické programy, programy pro projektová řízení, interní komunikaci či správu souborů ad.
- **Antivirové programy**
  > slouží k identifikaci, odstraňování a eliminaci počítačových virů
- **Podnikové informační systémy**
  > ERP neboli Enterprise Resource Planning slouží pro plánování podnikových zdrojů, ať už jde o materiál, finance, produkty, lidi ad.
- **CRM**
  > systém řízení vztahu se zákazníkem, respektive úložiště komplexních informací o klientech firmy

Vybavení firmy je velmi rozsáhlé a finančně tedy i poměrně náročné. Vysoké náklady potřebné pro zajištění chodu společnosti navíc v čase dále narůstají. Především kvůli nutnosti pravidelně obnovovat licence pořízených softwarových produktů a také z důvodu modernizace hardwarových komponentů.

Věděli jste, že firemní vybavení je nutné obměňovat přibližně každých pět let?

I proto stále více firem přechází na **cloudová řešení**, jako je třeba AlgoCloud od společnosti Algotech, kdy je provoz IT v maximální možné míře outsourcován zkušeným a spolehlivým partnerem. Zbavíte se tak povinnosti nakupovat speciální licence pro každého uživatele či zařízení zvlášť a současně se vám sníží náklady na pořízení nebo údržbu firemního hardwaru.

Přechodem na cloud kromě toho získáte i jistotu maximálního zabezpečení svých dat, která budou zálohována na několika místech a ukládána v souladu se všemi interními i legislativními normami, včetně nařízení GDPR.

Co je kybernetická bezpečnost

Kybernetickou bezpečnost je možné chápat jako soubor jasně stanovených opatření a pravidel, která mají za cíl zamezit nebo maximálně ztížit přístup k datům i síťovým prvkům firmy, při zajištění vysoké míry komfortu a bezpečí pro uživatele tohoto prostředí.

Podstatou kybernetické bezpečnosti je tedy ochrana informací před jejich krádeží či zneužitím. A to takovým způsobem, aby byla data nadále přístupná všem oprávněným uživatelům s minimem omezení. Nejde tedy pouze o technické zabezpečení, kdy je zajištěno zamezení přístupu neoprávněných osob k informacím, ale také o ochranu komunikačních cest proti spamu, malwaru, phishingu a jiným kybernetickým hrozbám.

Opomenout přitom nelze ani samotné zaměstnance společnosti. Velmi často jsou data zcizena či zneužita právě uživateli, kteří k nim mají zcela legitimní přístup v rámci výkonu své práce.

Z nejnovějších výzkumů vyplývá, že téměř tři čtvrtiny uživatelů odnášejí na nejrůznějších přenosových zařízeních týdně mimo firmu až 10 souborů!

Proto je v rámci zásad kybernetické bezpečnosti naprosto nezbytné dodržovat nejen platné legislativní standardy, ale také zavést jasně definované interní postupy pro práci s daty.

Co musí firmy a jejich zaměstnanci dodržovat?

1 Legislativa a regulatorní nařízení

V České republice je legislativní rámec tvořen především tzv. Zákonem o kybernetické bezpečnosti, který upravuje práva a povinnosti osob či působnost a pravomoci orgánů veřejné moci v této oblasti. Zpracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti komunikačních sítí i informačních systémů. Zákon byl v návaznosti na vývoj v oblasti ochrany dat několikrát novelizován, přičemž aktuální znění je účinné od 1. února 2020.

Významná novelizace tohoto zákona přitom proběhla již v roce 2017, kdy bylo nutné zajistit, že splňuje směrnici NIS platnou pro celou Evropskou unii. Co bylo jejím cílem? Směrnice zavedla jednotný standard v oblasti bezpečnosti sítí a IT systémů pro všechny státy EU a zásadně rozšířila povinnosti subjektů v oblasti ochrany a prevence před kybernetickými incidenty. Těmi jsou provozovatelé základních služeb a také poskytovatelé digitálních služeb, jako jsou internetové vyhledávače, online tržiště a cloud computing.

Významným legislativním opatřením je i Vyhláška o kybernetické bezpečnosti, která dále konkrétněji upravuje kupříkladu obsah a rozsah bezpečnostních opatření, náležitosti a způsob hlášení kybernetických útoků či způsoby jejich řešení.

Zatímco výše zmíněné legislativní náležitosti se dnes firmám a korporacím daří poměrně úspěšně dodržovat, novým strašákem se pro ně v roce 2018 stalo Obecné nařízení o ochraně osobních údajů neboli GDPR. Tato legislativa Evropské unie je v rámci kybernetické bezpečnosti naprosto zásadní. Pod pohrůžkou vysokých pokut totiž firmám nařizuje, že musí zajistit, aby se osobní data a citlivé údaje jejich zákazníků nedostaly do rukou nikoho dalšího.

Proč se nařízení stalo takovým strašákem? V případě GDPR neexistuje žádný mustr, podle kterého se musí všichni chovat. Každá společnost data uchovává jiným způsobem, a proto se na ni vztahují pravidla dle konkrétního případu. Bez rady a pomoci odborníků se v tomto případě tedy neobejde nikdo.

2 Interní předpisy

Data jsou prakticky v každé společnosti jedním z nejdůležitějších aktiv. Proto také firmy investují nesmírné finanční prostředky do zabezpečení infrastruktury pro jejich ochranu. Často však zapomínají na své zaměstnance, kteří s daty na denní bázi pracují. Kromě útoků externích narušitelů totiž mohou jejich únik často, ať už úmyslně či neúmyslně, způsobit právě sami pracovníci.

Nezapomínejte proto ani na interní předpisy, které pro práci s informacemi nastaví jasná pravidla a určí všem zaměstnancům povinnosti vyplývající z platné legislativy i jejich pracovní náplně. Jak by měly vypadat? Aby byly interní předpisy v oblasti kybernetické bezpečnosti kvalitní, musí v nich být precizně – avšak srozumitelně – předepsané pokyny, kterými se mají zaměstnanci řídit. Neměly by proto obsahovat složité definice či převzaté povinnosti ze zákona. Kromě organizačních opatření by pak každá společnost měla mít vytvořené i školící instrukce a krizové plány pro případ jejich porušení.

Nejste si jistí, zda vaše společnost splňuje veškerou platnou legislativu nebo byste si rádi nechali provést bezpečnostní analýzu?

Obraťte se na specialisty ze společnosti Algotech, která spravuje počítačovou bezpečnost řady velkých institucí, stejně jako malých a středních podniků. Provedou u vás detailní bezpečnostní audit a pomohou vám s odstraněním nalezených slabých míst či nedostatků, a to včetně proškolení zaměstnanců ohledně aktuálních kybernetických hrozeb.

Jsou firmy dostatečně chráněné?

Kybernetické útoky představují pro firmy obrovský problém. Se stále chytřejšími technologiemi přicházejí nové způsoby a metody jejich napadení. Útoky jsou komplexnější a hackeři jsou ve svých aktivitách mnohem sofistikovanější. Obyčejný antivirový program dnes už nestačí.

Firmy proto své zabezpečení nemohou podceňovat! Ztráta i jen několika dokumentů může společnost a její pověst nenávratně poškodit v očích veřejnosti i klientů. O to více, když za zcizením či zneužitím dat a citlivých údajů stojí samotní zaměstnanci.

Podle Petra Loužeckého ze společnosti Algotech nejsou informační systémy ve většině tuzemských firem v optimální kondici. Na vině nejsou jen zastaralé informační systémy, ale i časté podcenění rizik a nedostatečné nastavení úrovně zabezpečení. *„České firmy jsou chráněny velmi špatně. Zatímco velké nadnárodní korporace, jako jsou banky či pojišťovny, mají ochranu svých dat na velmi slušné úrovni, u menších firem tomu tak není. A naprosto dokonalé zabezpečení nemá prakticky nikdo,“* vysvětlil.

Nejhůře jsou na tom co se týká ochrany dat malé a střední firmy. Tedy společnosti, které mají 50–250 zaměstnanců, využívají vlastní IT vybavení, technologie i aplikace a snaží se pracovat tzv. „z terénu“ pomocí vzdálených přístupů do firmy. *„Většina těchto firem se spokojí s úplným minimem, jako je antivirový program, protože investice v řádu několika milionů korun do kybernetického zabezpečení jim nedává smysl. Právě proto jsou tyto podniky nejohroženější. Neuvědomují si jednu věc – kybernetické hrozby nejsou jen o tom, že jim někdo ukradne data či know-how. Cílem útoků je ve většině případů spíše zašifrování či zavirování firemní sítě a znemožnění dané společnosti vyrábět nebo se věnovat podstatě svého podnikání. A tento stav může trvat několik dnů, nebo dokonce týdnů,“* vysvětlil dále Petr Loužecký. Firma je tak naprosto ochromena a přichází o zisk.

Tuto skutečnost potvrzují i nejnovější data Českého statistického úřadu, dle kterých kybernetických útoků v Česku přibývá. Jenom za minulý rok čelilo kybernetickým útokům více než 80 % českých firem. Nejčastěji přitom šlo o útoky s cílem přehltit kapacitu serverů velkým množstvím požadavků (DDoS) nebo o vyděračské programy, které způsobují nedostupnost dat, a za jejich obnovení požadují výkupné. S těmi se setkala téměř třetina velkých a čtvrtina středně velkých firem působících na území České republiky. Další pětina firem pak čelila zničení nebo poškození dat.

Nejčastější kybernetické hrozby

Phishing a spear phishing

Nejobvyklejší cestou, jak se do firmy dostane škodlivý vir, je přes e-mail.

Zaměstnanci jsou během pracovní doby často zaneprázdnění, věnují se klientům, chodí na schůzky nebo vyřizují běžnou agendu. Díky tomu se mohou stát snadnou obětí tzv. phishingu a spear phishingu. O co jde?

Tradiční **phishing** představuje typicky rozesílání obrovského množství e-mailů s prolinkem náhodným příjemcům, od nichž se útočníci snaží získat přihlašovací údaje a hesla do firemních systémů. Přestože je tento typ útoku obvykle odhalen antivirovým programem, v případě nepozornosti může zaměstnance zmást. Přichází totiž od zdánlivě známé osoby či instituce.

V případě **spear phishingu** jde o útok cílený. Útočníci zašlou e-mail konkrétní osobě, která je většinou ve firmě vysoce postavená. Takto zaslaný e-mail je těžko odhalitelný antispamovým filtrem, jelikož se vyskytuje pouze v malém množství a nevykazuje typické znaky tradičního phishingu. V e-mailu není uveden prolink, je obvykle psán perfektní češtinou a obsahuje přílohu se škodlivým kódem, která není detekována antivirem.

Malware

Pomocí výše zmíněných typů podvodných e-mailů se mohou do firemních zařízení (počítačů i telefonů) velmi snadno dostat škodlivé programy, které jsou označovány jako malware. Jejich úkolem je poskytnout útočníkovi příležitost vzdáleně ovládat dané zařízení, snížit výkon systému, nakazit síť, případně získat přístupová hesla, kopírovat a měnit obsah uložených dat či sledovat interní komunikaci.

Typů malwaru je opravdu mnoho – mezi nejznámější patří v současnosti především viry, červy, trojské koně, adware, ransomware a spyware. Jaký je mezi nimi rozdíl?

Virus se šíří bez vědomí uživatele tak, že se množí do nejrůznějších systémů a programů. **Trojský kůň** zase poskytuje hackerům přístup do systému. Nedokáže však sám infikovat další počítače nebo programy svojí kopií. Proto existují tzv. **červy**, které na napadeném zařízení instalují trojské koně nebo je vytvářejí z již nainstalovaných programů. **Adware** pak uživatele obtěžuje nekonečnou záplavou vyskakovacích oken s reklamou. Většina těchto programů nepředstavuje riziko, některé však dokážou shromažďovat osobní informace nebo nahrávat stisknuté klávesy. Podobně pak funguje i **spyware**, který je určen ke špehování. Skrývá se na pozadí a shromažďuje citlivé informace, jako jsou přihlašovací údaje a hesla. A může také hackerovi poskytovat vzdálený přístup do firemních zařízení.

Ransomware

Jednou z nejaktuálnějších a nejrozšířenějších kybernetických hrozeb se v posledních letech stal především ransomware, který je překládán jako vyděračský software. Jeho úkolem je napadnout počítačový systém firmy a zašifrovat v něm uložená data. Následně pak útočník požaduje od oběti výkupné za obnovení přístupu k nim. Ve většině případů obsahuje i konkrétní časový limit, po jehož uplynutí jsou data nenávratně smazána.

Jelikož však firmy při řešení této situace v minulosti obvykle zaujaly postoj: „S vyděrači se nevyjednává!“, hackeři tento útok zdokonalili. Již nehrozí pouhým smazáním dat, ale naopak jejich zveřejněním na internetu. Protože ztracená data mohou obsahovat kromě citlivých údajů i interní know-how, může mít útok skutečně devastující účinky. A netýká se zdaleka jen velkých korporací. Dle aktuálních průzkumů útočí hackeři v České republice především na malé a střední firmy.

Nejnebezpečnější útoky tohoto typu měl na svědomí kupříkladu ransomware WannaCry, který v květnu 2017 napadl více než 250 000 počítačů a za odemknutí dat požadoval po uživatelích až 46 000 Kč. V prosinci 2018 zase byly programem Ryuk paralyzovány nemocnice v Benešově a hutní společnost OKD. Kromě toho, že je útok vyřadil na dlouhou dobu z provozu, musely obě společnosti vynaložit na obnovu systémů finanční prostředky v řádu desítek milionů korun.

„Státní správa je v tomto případě ukázkovým příkladem toho, jak je snadné se do systému instituce dostat. Její zaměstnanci technologiím vůbec nerozumí, což po nich ani nikdo nemůže chtít. Mají odlišnou agendu i starosti. Ale v tomto leží největší slabina státních orgánů a vlastně i malých a středních firem – jejich zaměstnanci jsou důvěřiví. A v rámci toho, že se snaží svou práci dělat dobře, tak otevírají naprosto vše, co v rámci online komunikace obdrží,“ vysvětlil Petr Loužecký z Algotechu.

Máte svá data a systémy v bezpečí?

U všech kybernetických hrozeb platí, že největší úspěchy mají útočníci cílící na nejslabší článek řetězce. Tím je nejčastěji právě nesoustředěný zaměstnanec. K vpuštění do systému pak stačí jedno jediné kliknutí.

Investice do zabezpečení je proto potřeba chápat jako nezbytný náklad, který musí firma v rámci svého podnikání vynaložit, pokud chce obstát v současném vysoce konkurenčním prostředí. Většina kybernetických útoků v soukromém sektoru totiž není vedena cíleně, nýbrž plošně. To znamená, že útočníkovi je vcelku jedno, jakou konkrétní firmu napadne, neboť primárně hledá vysoce zranitelné systémy, do nichž se dokáže snadno dostat.

Kyberkriminalita v České republice navíc roste. Zatímco v roce 2011 evidovala Policie ČR zhruba 1 500 případů počítačové kriminality, o osm let později už jich registrovala více než 8 000. To představuje nárůst o 430 %! Skutečná čísla jsou však úplně jiná. Odborníci se domnívají, že počet nehlášených podvodů a pokusů o zcizení dat dosahuje spíše několika stovek tisíc případů. Řada firem také pokus o útok ani nemusí zaznamenat a dozvídá se o něm až zpětně při provádění bezpečnostních auditů svých IT systémů.

Každá firma by proto měla IT systémy a data zajistit jak fyzicky, aby je nemohl nikdo odnést, tak i virtuálně na úrovni firewallů, antivirových nástrojů, nástrojů na sledování sítě či pohybu dat v síti (DLP). S tím souvisí, že se každá společnost musí zaměřit na dvě věci – zálohování dat a školení uživatelů. Zálohy by přitom měly být nejen časté, ale i kompletní, aby z nich šla „firma“ skutečně obnovit a netrvalo to týdny. Jednou z forem je zálohování dat do cloudu, případně vytvoření záložního prostředí celé firmy v cloudu. *„Všechny zákazníky i zaměstnance je pak potřeba neustále poučovat o tom, jaké hrozby plynou z toho, že porušují základní pravidla kybernetické bezpečnosti,“* vysvětlil Petr Loužecký z Algotechu k nutnosti průběžného proškolování uživatelů. Pomůže jim to totiž pochopit rizika spojená s hesly, využíváním veřejných Wi-Fi sítí, neautorizovaným stahováním programů ad.

Kde začít aneb odhalení hrozeb

Pamatujte si: V případě kybernetických útoků je prevence finančně mnohem méně nákladná, než následné odstranění jejich důsledků.

Útočník je proti firmě ve výhodě. Zatímco jemu stačí nalézt jedinou skulinku či slabinu, skrze kterou do firmy pronikne, samotná společnost je musí najít a následně odstranit naprosto všechny. Z tohoto důvodu by si každá firma měla nechat udělat **audit kybernetické bezpečnosti**, který odhalí její slabá místa, definuje nejhodnotnější aktiva společnosti, jakým hrozbám jsou vystaveny, případně jak může být tato zranitelnost jinak zneužita.

Audit kybernetické bezpečnosti se dá udělat i svépomocí, ale je to pro firmu velmi náročné – ať už z hlediska času nebo personálního zajištění. *„Dnes je obor IT natolik složitým odvětvím, že se každý člověk specializuje pouze na jednu jedinou oblast, ve kterém je naprostým expertem. Firma by proto pro provedení kvalitního auditu kybernetické bezpečnosti potřebovala až pět lidí, kteří mají velmi hlubokou znalost dané oblasti implementace kybernetické bezpečnosti a jsou schopni analýzu provést naprosto objektivně,“* vysvětlil Petr Loužecký z Algotechu. Jinými slovy, jeden člověk dnes prostě nemůže mít takové know-how, aby jím provedený audit bezpečnostních rizik přinesl firmě dostatek informací.

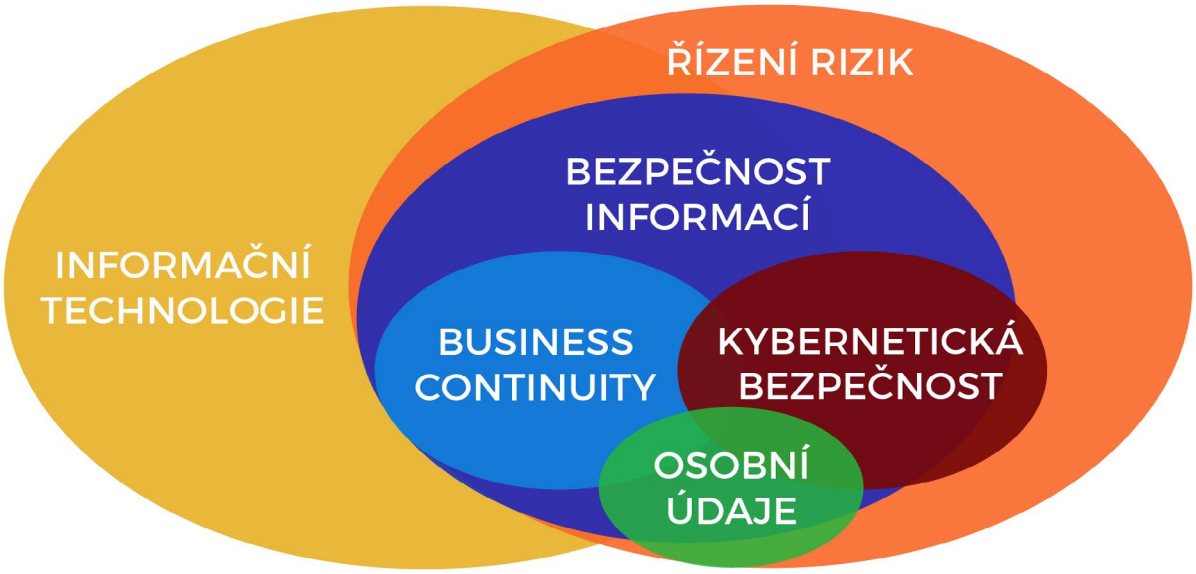
Často se pak stává, že firma začne implementovat zásady kybernetické bezpečnosti „bez ladu a skladu“. To je ale naprosto k ničemu, protože neví, co má vlastně chránit, případně jaké investice do ochrany je potřeba udělat. *„V praxi často vidím, že firma nakoupí různá zařízení a softwary na ochranu uvnitř firmy, ale data, která jsou pro ni až životně důležitá, si zaměstnanci i vedení vzájemně sdílí přes internet nebo aplikace třetích stran,“* upozornil Petr Loužecký.

Implementace zásad kybernetické bezpečnosti nemusí zachránit nic, pokud firma neví, co konkrétně je potřeba chránit.

Mnohem větší smysl proto dává **externí audit kybernetické bezpečnosti**, kdy firmu zkontroluje člověk zvenčí, který není zaujatý nebo zatížený historií společnosti či vztahy na pracovišti. Pouze takovýto člověk může objektivně poukázat na nedostatky v procesech nebo technologickém zabezpečení, upozornit na rozpory mezi platnými předpisy i praxí a hlavně otevřít diskuzi na úrovni managementu nad směřováním implementace kybernetické bezpečnosti v dané společnosti.

„My děláme audit tak, aby z něj firma měla prospěch. IT oddělení od nás proto dostává argumenty pro management k tomu, co je potřeba dělat jinak, jaké vybavení a zabezpečení je třeba nakoupit či jak je nutné změnit pravomoci. Jsme pro něj spojencem a snažíme se mu poradit, jak může svou práci dělat efektivněji. Proaktivně také pomáháme zlepšovat zabezpečení, aby IT oddělení nemuselo řešit následné úniky,“ odhalil přístup společnosti Algotech Petr Loužecký, který řeší kybernetickou bezpečnost v rámci produktu AlgoCloud.

Obrázek: Vztah mezi řízením rizik, kybernetickou bezpečností a ochranou osobních dat



Jak se ochránit?

Na základě konkrétních zjištění externího auditu kybernetické bezpečnosti si může následně firma stanovit priority a zavést s pomocí dalších odborníků odpovídající bezpečnostní opatření. Ty se přitom liší podle toho, zda chce firma s pomocí expertů zajistit fyzickou i virtuální bezpečnost svých dat v rámci vlastní IT infrastruktury a systémů, nebo se na základě auditu rozhodne přesunout svá nejcennější aktiva do bezpečí profesionálního datového centra.

Zabezpečení v rámci vlastní infrastruktury se v zásadě skládá ze čtyř na sebe návazných kroků, které si může firma zajistit svépomocí, nebo je svěřit do rukou odborníků, jejichž znalosti jim ušetří nejen čas, ale i peníze. Co je tedy nutné udělat?

1 Chraňte svá zařízení

Bez funkčního vybavení nemůže firma fungovat, a tedy ani generovat zisk. Proto je třeba zajistit, že veškerá IT infrastruktura používá nejaktuálnější verzi softwaru i antivirových, antimalwarových a antispamových programů. Ujistěte se, že lokální i bezdrátové sítě jsou zabezpečené firewallem a zaměstnanci se seznámili se zásadami používání firemního vybavení i bezpečnostními funkcemi, které musí obsahovat. Obzvlášť pokud notebooky, mobilní telefony a další elektronická zařízení používají i mimo pracoviště. *„Zaměstnanci firem teď pracují z domova, často ze svých soukromých počítačů, kde je těžší zkontrolovat vhodnost a účinnost zabezpečení. Klienti od nás proto dostávají i instrukce, jak postupovat při nastavení vzdálené kanceláře,“* zmínil Petr Loužecký ze společnosti Algotech. Bezpečnost totiž dle něj není jen o kvalitních IT systémech, ale především o nastavení procesů uvnitř organizace a řádně vedené dokumentaci.

2 Chraňte svá data

Naprosto každá firma musí mít svá data v bezpečí – ať už jsou v centru jejího podnikání, nebo ne. V první řadě je proto nutné veškeré životně důležité informace zálohovat. A to tak, že je při ztrátě dat možné ze záloh celou firmu v řádu hodin zase obnovit a uvést do provozu. *„Zejména pro klienty s osobními či citlivými údaji je opravdu důležité, aby zaměstnanci důsledně dodržovali pokyny kybernetické bezpečnosti a všechna data zálohovali. Ideálně na vzdálené úložiště – cloud,"* popsal Petr Loužecký ze společnosti Algotech. Ujistěte se také, že je veškerá firemní komunikace šifrovaná a máte správně nastavenou správu i ověření uživatelů a jejich práv. Víte, kdo všechno má ve firmě přístup k citlivým informacím? Proaktivně chraňte elektronická data pomocí technologie DLP (neboli Data Leak/ Loss Prevention). Můžete díky ní omezit přístupy na hardware nebo ji nasadit jako tajného klienta do firemních zařízení či na serverech, kde bude kontrolovat činnost uživatelů, případně blokovat nežádoucí aktivity.

3 Chraňte data svých klientů

Ztráta dat znamená ohrožení byznysu. Odcizení dat a citlivých údajů zákazníků a klientů však nadto přináší i závažné právní důsledky! Pokud totiž nepracujete v souladu s velmi přísnou směrnicí GDPR, která zavádí obrovské restrikce, regulace a povinnosti při práci s osobními údaji bez výjimky pro všechny firmy, čekají vás mnohamilionové pokuty! Nechte si proto provést audit GDPR od společnosti Algotech. Experti na tuto legislativu projdou vaše firemní zabezpečení, interní procesy, technické zázemí i používané technologie. Nejenže vám pomohou odhalit všechny nedostatky, ale souhrnně vám předloží i možnosti jejich nápravy. A to za relativně nízké náklady.

4 Zajistěte si bezpečnostní dohled

Čím více a lépe se v dnešní době firmy chrání, tím vynalézavější dokážou být hackeři v tom, jak tyto ochrany překonat. Firmy by proto v žádném případě neměly podceňovat ani bezpečnostní dohled (SOC). Toho lze nejsnadněji dosáhnout pomocí bezpečnostního operačního centra, které provádí nepřetržitý monitoring aktivit v síti. Jeho úkolem je hledat, identifikovat a případně informovat o potenciálně škodlivém chování ve firemní IT infrastruktuře. Díky tomu se výrazně snižuje riziko toho, že se firma o úniku či zneužití dat dozví až ve chvíli, kdy je na jakékoliv bezpečnostní opatření pozdě.

NEBO...

Přejděte do cloudu

Je tady však mnohem jednodušší a levnější cesta k zajištění firemní kybernetické bezpečnosti. Tím je **přechod do cloudu**. Veškerá zodpovědnost týkající se zabezpečení dat leží v tomto případě plně na poskytovateli služeb datového centra, v němž jsou vaše aktiva uložena. Cloud představuje v zásadě nedobytnou pevnost – nelze se do ní dostat ani fyzicky, ani virtuálně. Datové centrum tvoří zabezpečené a střežené budovy, které jsou postavené a certifikované speciálně pro poskytování služeb cloudu. Podléhají navíc nejen legislativě České republiky, ale také Evropské unie. *„Pokud se na to podíváme z pohledu investic, je to jednoznačně ta nejlevnější varianta. Za měsíční poplatek získáte unikátní souhrn technologií a služeb, díky kterým máte jistotu maximálního zabezpečení svých dat. Přechodem do cloudu se zbavíte povinnosti nakupovat speciální licence pro každého uživatele či zařízení a současně se vám sníží náklady na obnovu hardwaru i softwaru až o 40 %,“* objasnil Petr Loužecký z Algotechu.

Cloud a bezpečnost jsou spojené jako vztah a důvěra

Cloud musí splňovat veškerá bezpečnostní opatření, která malé a střední firmy nejsou často na svých pobočkách schopna dodržet, ať už z hlediska nutných investic do vybavení, nedostatku odborníků či pouhého podcenění rizik. Právě pro tyto malé a střední firmy, které nemají dostatek prostředků na zajištění naprosto všech oblastí kybernetické bezpečnosti, je cloudové řešení ideální. Zaručuje totiž nejen technologickou stránku věci, ale i tu legislativní. *„V Algotechu jsme se začali kybernetickou bezpečností zabývat velmi intenzivně v návaznosti na poskytování cloudu. Vycházíme také z unikátního know-how, které jsme v rámci GDPR auditů získali ze spolupráce s více než 250 firmami. A nyní jej procesně přenášíme do kybernetiky, protože osobní údaje jsou ve své podstatě podmnožinou dat. Pohled na ně je velmi podobný, liší se jen technická míra opatření,“* objasnil Petr Loužecký.

Už jste se rozhodli?

Nebuďte firmou, která říká: „Nám se to stát nemůže!“ Věnujte ochraně svých dat péči, kterou si zaslouží. A ať už se rozhodnete v rámci implementace kybernetické bezpečnosti pro jakoukoliv cestu, nechte si pomoct od expertů. Ušetří vám čas a zajistí, že vás ochrana dat nebude stát zbytečné peníze.

„Přechodem do AlgoCloudu získáte jistotu maximálního zabezpečení svých aktiv. Veškerá data zálohujeme na několika lokalitách a v případě potíží jsme schopni je obratem obnovit,“ uvedl Petr Loužecký a dodal: *„Jelikož ale chceme našim klientům poskytovat komplexní servis, jsme schopni dostat kybernetickou bezpečnost v rámci aktuální nabídky také na zákaznickou lokalitu – tedy až před dveře dané společnosti.“*

algotech