ELEKTRONICKÝ

SPEDIČNÍ ZPRAVODAJ

VII/2021

SVAZ SPEDICE A LOGISTIKY ČESKÉ REPUBLIKY
Zapsaný spolek
ASSOCIATION OF FORWARDING & LOGISTICS
OF THE CZECH REPUBLIC-MEMBER OF FIATA

Obsah:

info@svazspedice.cz
Sekretariát Svazu spedice a logistiky ČR, z.s.
1.pluku 8a, 18630 Praha 8 – Karlín
tlf. 224 891 303
Internet: www.svazspedice.cz

TÉMA: Kyberkriminalita

1. Úvod

Malé a střední podniky si stále více uvědomují často jejich existenci život ohrožující důsledky kyberkriminality. Přesto se však o ní stále příliš zřídka diskutuje otevřeně, a přitom kybernetická bezpečnost je na programu každé velké logistické akce.

Výkonní ředitelé a manažeři raději informují o úspěších ve spolupráci s novým klientem, než o důsledcích útoku ransomwaru. Jsou to však právě ti, kteří by se měli touto otázkou otevřeně zabývat, aniž by se obávali stigmatizace jako oběti. Kdo není postižen, může být potěšen, že byl dosud ušetřen. Jak dlouho taková radost potrvá, není jisté. Problém může zasáhnout kohokoliv.

Jde tedy o bezvýhradné šíření a diskusi účinných přístupů, které chrání před kyberkriminalitou. Je mnoho bodů, o kterých stojí za to diskutovat: Jak dosáhnout co nejlepší ochrany IT systémů? Co dělat, když došlo k útoku hackerů? Měli byste v případě vydírání zaplatit výkupné, nebo raději ne? Jaké pojistné krytí je užitečné a jaká rizika jsou ohrožena? Širší diskuse o tom by mohla pomoci; proto jedno z posledních vydání DVZ e-Bulletinu bylo věnováno tomuto tématu.

2. Kyberzločin – existenční riziko

Kybernetické útoky představují pro logistické společnosti velké riziko. Silné vnitřní propojení odvětví a rostoucí využívání digitálních aplikací nabízí pachatelům trestné činnosti širokou škálu vstupních míst. Hackerské útoky na logistický průmysl narůstají a podle zprávy německého Federálního úřadu pro vyšetřování trestné činnosti (Bundeskriminalamt Wiesbaden) se loni počet útoků zvýšil o 7,9 procenta na přibližně 108 000.

Odborníci však očekávají vysokou úroveň utajení. Zločinci mají velkou šanci, že budou ignorováni.

Pouze jedna třetina případů byla vyřešena. „Rizika kybernetických útoků na logistické společnosti jsou větší než před dvěma až třemi lety a jsou nyní v první trojce," říká Frank Ewald, bezpečnostní manažer Deutsche Post DHL, který se nedávno se zúčastnil Dne prevence digitální trestné činnosti (DVZ).

Zejména útoky ransomwarem jsou pro společnosti nebezpečné. Škodlivý software propašovaný jako cíl kyberzločinu do firmy a někdy blokující IT infrastrukturu na týdny nebo měsíce. Pak hackeři zašifrují data a požadují výkupné za jejich následné dešifrování. Takové útoky mohou podnikání firem výrazně omezit, a někdy dokonce úplně zastavit. Je proto naprosto nezbytné mít přístup k zálohování všech údajů.

3. Pojištění kybernetického rizika

Stále větší počet malých a středních podniků uzavírá pojištění proti útoku hackerů, říká Richard Renner, generální ředitel Schunck Group. Jeho pojišťovna již v červnu letošního roku uzavřela v tomto segmentu podobný objem pojistných smluv jako za celý loňský rok. Zejména ve velkých domech je dnes bezpečnost proti kybernetickým útokům standardní. Podle Rennera by management riskoval případ odpovědnosti za škodu, pokud by nebyl schopen tuto záležitost prokázat a strukturovat.

Otázka však spíše zní: kdy?

Logistickou společností, na kterou letos zaútočili hackeři, je spediční skupina Ulmer Noerpel. „Na veřejnosti se o kybernetické bezpečnosti a hackerských útocích příliš otevřeně nemluví," říká Judith Noerpel-Schneiderová, Člen výkonné rady.

O zkušenostech své společnosti informovala na Dni digitální prevence kriminality. Hovořila s mnoha firmami, které byly také postiženy, a došla k závěru, že to není otázka samotného napadení, ale kdy a v jakém rozsahu nastane. „Problém musíme řešit jako manažeři, abychom minimalizovali škody v případě útoku hackerů", zdůrazňuje paní Noerpel-Schneiderová.

Ke kybernetickým útokům může docházet s různou kriminální motivací. Kromě útoků s ransomware a následného nátlaku na výkupné mohou hackeři za účelem jejich zneužití

vyhledávat osobní údaje a přístupová práva. Tomu se říká krádež identity. Dalším zločinným záměrem je například manipulace s počítačovými systémy, aby je mohli dálkově ovládat. Hackeři je pak mohou připojit k podřízeným sítím a provést další velké kybernetické útoky.

4. Jak postupovat v případě napadení

Když se společnost stane obětí kybernetického útoku, je důležité jednat rychle a přijímat rozhodnutí na úrovni vedení. Například, je třeba okamžitě uvědomit Policii, Úřad pro ochranu dat a Pojišťovnu. Společnosti provozující kritickou infrastrukturu podle zákona o bezpečnosti informačních technologií musí v Německu navíc incident nahlásit Spolkovému úřadu pro bezpečnost v informačních technologiích (BSI).

Podle paní Noerpel-Schneider je také nezbytné okamžitě svolat krizovou štáb, který připraví havarijní plány. „Složení krizové jednotky musí být definováno předem. Musí existovat jasná obsahová pravidla pro interní a externí komunikaci, například se zákazníky, která musí být přísně uplatňována. Na tohle by měl být zřízen a připravován manažer pro krizovou komunikaci.

Zvlášť choulostivý moment je vyděračský odkaz, který přináší ultimátum pro řešení požadavků na výkupné. Rozhodnutí, zda společnost ustoupí požadavkům vyděračů, je často spojeno se situací v záloze. Kromě toho je klíčová otázka nákladů na prostoje, pokud je IT-systém dlouhodobě zablokován a obchodní procesy nefungují vůbec nebo pouze v omezené míře. Vlastní žádost o výkupné se pak obvykle uplatňuje prostřednictvím vyděračského spojení.

Paní Noerpel-Schneider v tomto ohledu doporučuje zvážit, zda se má vydíraný vyděračům podvolit, protože když to udělá, začne okamžitě běžet lhůta pro úhradu. A pokud to nebude respektováno, vyděrači zvýší svou poptávku.

Úplný rozsah škod a přijatá opatření by měly být přesně zdokumentovány, doporučuje paní Noerpel-Schneider. To, jak k tomu dojde, by mělo být zahrnuto do nouzového plánu. Je také užitečné mít profesionální forenzní tým a spolupracovat s pojišťovnou.

Za účelem ochrany před útoky hackerů a snížení škod v případě vstupu by IT-specialisté měli pravidelně provádět komplexní bezpečnostní kontrolu. To může zahrnovat tzv. penetrační testy, které se aktivně pokoušejí proniknout do podnikové sítě s cílem odhalit nedostatky v IT prostředí. Mezi další opatření může patřit segmentace prostředí systému a možnost odříznutí provozních systémů od klientů.

Součástí filosofie vybudování záložní infrastruktury a bezpečnostní strategie je předpokládat, že IT systém může být ohrožen kdykoli. Proto je aktivní monitorování architektury IT užitečné pro co nejrychlejší identifikaci podezřelých procesů.

Tuto službu by mohli provést i externí poskytovatelé bezpečnostních služeb. Rovněž je třeba kontrolovat, zda jsou zálohy prováděny pravidelně. „Dobrá záložní infrastruktura se vyplatí, protože umožňuje začít znovu rychle podnikat," říká paní Noerpel-Schneider. „Nouzový koncept je velmi důležitý. Od počátku musí být jasné, které jsou časově kritické obchodní procesy a jak mohou být realizovány v nouzových operacích, a to i bez IT. Jakkoli to může znít neobvykle ve věku digitalizace: Dokumentace a plány prostředí IT systému by měly být někde vytištěny na papíře".

5. IT-Security ve firmách

Protože společnosti nejsou před kybernetickými útoky v bezpečí, i když podnikají tak rozsáhlá opatření, měly by zvážit uzavření kybernetického pojištění. Některé pojišťovny vysílají specialisty, kteří pomáhají omezit škody. A konečně, podle paní Noerpel-Schneider je velmi důležité pravidelně školit personál a zvyšovat povědomí o bezpečnosti IT a uplatňovat chování ve firmě v případě nouze.

Vzhledem k rostoucímu riziku jsou požadavky na strategii IT-Security stále náročnější, také proto, že přidaná hodnota společnosti je znásobena digitalizací a význam dat se zvyšuje. V souladu s tím by škody způsobené útoky hackerů mohly být stále větší, říká Christian von Rützen, odpovědný za provádění strategie IT v Dachseru.

Kyberzločinci jsou vždy o krok napřed se svými metodami a útočnými vzorci. „Obránci jsou často poraženi," říká Matthias Vallentin, zakladatel a generální ředitel IT bezpečnostní agentury Tenzir v Hamburku. Porovnáme-li prostředí IT s oploceným pozemkem, musíme podle Vallentina chránit celý plot, a nejen hlavní vstupní bod. Rychlost útočníků se navíc výrazně zrychluje. „Zneužití zranitelnosti trvá jen několik hodin," poznamenává Vallentin. Bezpečnostní mezera se proto musí vhodnými záplatami odstranit nejpozději do 72 hodin.

6. Závěr

Útočníci jsou někdy aktivní na firemní síti celé měsíce, než například zašifrují data a podají žádost o výkupné. V této době, „napadený je zdaněn," říká von Rützen. Hodnota údajů, k nimž mají zločinci přístup, určuje požadavek na výkupné za společnost.

Von Rützen v této souvislosti zdůrazňuje, že preventivní přístup jako bezpečnostní strategie nestačí. Ve skutečnosti byste měli vždy předpokládat, že by vás mohli „hacknout". V době, kdy se útočníci teprve rozhlížejí po firemní síti a shromažďují informace, má dle Vallentina společnost stále šanci vypořádat se s kyberzločinci, než dojde k větším škodám.

Delikátní je také otázka, zda výkupné má být za určitých okolností zaplaceno, nebo zásadně nemá. „Je to pochopitelné, ale ve společenském kontextu zničující," říká Richard Renner, generální ředitel Insurance Schunck Group. Skutečnou odpovědí musí být neplatit. Společnost, která platí, riskuje, že bude znovu a znovu vydírána, protože v určitých kruzích dostane cejch slabocha.

Někteří odborníci na bezpečnost se staví odmítavě k návrhům legislativního zákazu úhrady výpalného. „Už jen tento krok by byl jednostranný," říká pan Ewald z DHL. Pokud by taková nařízení existovala, společnostem by se v případě vydírání muselo pomoci obnovit činnost, aniž by zaplatily výkupné. Podle Ewalda by vlády musely zajistit dodatečnou bezpečnostní infrastrukturu, kterou by mohly dotčené společnosti a organizace využívat.

V USA jsou pravidla mnohem přísnější. „Když tam zaplatíte výkupné, musíte počítat s obviněním z financování terorismu a skončit na seznamu státních teroristů," říká Niels Beuck,

vedoucí bezpečnostní politiky ve Spolkové dopravní a logistické asociaci DSLV. Za těchto okolností zúčastněné strany dvakrát zvažují, zda skutečně zaplatí.

Podle IT bezpečnostního experta Vallentina, asi 30 procent pokusů o vydírání skončí zaplacením výkupného. To samozřejmě, jak uvedeno výše, závisí na právních požadavcích příslušné země. Jedna věc však musí být zúčastněným jasná:

Výplata výkupného není zárukou, že vše bude dále probíhat jako před útokem. Existuje riziko, že údaje budou neúplné a IT-infrastruktura zůstane poškozena. Tak či onak, bohužel zatím neexistuje způsob, jak vytvořit skutečně bezpečné zálohy.

Konec VII. čísla

Příjemné pokračování rozvolňování vám přeje Redakce SZ SSL