N-ABLE™

ZEBRA SYSTEMS

Endpoint Detection and Response:

Jak demonstrovat návratnost investice

eGuide

Úvod

Pandemie značně změnila způsob, jakým vykonáváme každodenní činnosti. Lidé tráví více času online prací, nákupy, virtuálními eventy, a dokonce i lékařskými vyšetřeními. To nutí organizace urychlit svůj přesun ke cloudovým službám. Když k tomu přičtete ještě práci z domova a používání vlastních zařízení, vychází z toho vyšší množství možných vektorů útoku.

Úkolem MSP je spravovat a chránit zařízení, data a procesy jejich zákazníků, takže často mají široký přístup k jejich systémům. To dělá z MSP a nástrojů které používají lákavý cíl útoků. Nedávný průzkum od N-able[1] zjistil, že 90 % MSP se od začátku pandemie začíná stále více stávat primárním cílem útoků – a nevypadá to, že by tento trend zpomaloval.

Během několika posledních let jsme mohli být svědky rychlé adopce systémů detekce a reakce pro koncové body (EDR) mezi MSP. Stále více poskytovatelů služeb přechází od klasických antivirových řešení[2] k EDR, ale často se setkávají s odporem ze strany svých zákazníků, kteří nechtějí změnu, a dostávají se tak k výzvě demonstrovat návratnost investice (ROI).

V tomto eGuidu se podíváme na nejlepší způsoby, jak se s touto výzvou vyrovnat a jak produktivně diskutovat o EDR se svými zákazníky.

Jak nejlépe demostrovat ROI u EDR

Ačkoliv na první pohled může jít o téměř nesplnitelný úkol, promyšlený systematický přístup jej může značně usnadnit.

1. Vysvětlete klientům všeobecnou situaci v kybernetické bezpečnosti
2. Snažte se pochopit jejich potřeby a náhled na problematiku
3. Ukažte jim škodu způsobenou útokem na reálných příkladech
4. Navrhněte své bezpečnostní řešení a plány na jeho zavedení
5. Pokud budete stále mít problém řešení prosadit, navrhněte zákazníkovi úpravu zopovědnosti za bezpečnost jeho infrastruktury

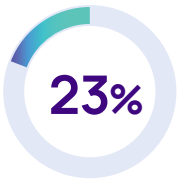
Projděme si tedy klíčové body ke každému z uvedených kroků.

1 Poskytněte svým klientům přehled o současném stavu kybernetické bezpečnosti

Jednoduchá statistika může mít velký dopad pro ilustraci aktuální situace. A pokud statistika nebude dostatečně přesvědčivá, titulky zpráv o posledních únicích dat pomohou objasnit pointu vašim zákazníkům. Například takto:

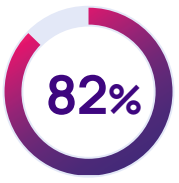
105%

Ransomware dosáhl nových rekordů v roce 2021 se 105% nárůstem oproti roku 2020[4].



23% incidentů s únikem či poškozením dat bylo způsobeno lidskou chybou[5]

42% nejčastějších útoků se kterými se MSP setkávají zahrnují ransomware[6]



82% zákazníků MSP se setkalo s nárůstem počtu pokusů o kybernetické útoky[7]

Vaším cílem není zákazníky vystrašit, ale pomoci jim porozumět tomu, že všechny firmy, ať už malé nebo velké, mohou být cílem útoku a utrpět vážné škody. Proto je potřeba pečlivě vybrat řešení, které bude schopné držet krok s hrozbami.

2 Snažte se pochopit jejich potřeby a perspektivu

Ujistěte se, že jste pochopili potřeby a požadavky zákazníka. Abyste zjistili, na čem jim opravdu záleží a jaké řešení pro ně bude nejlepší, zeptejte se na jejich cíle a předpoklady o jejich dosažení. Zde je pár otázek pro začátek:

- Byla vaše firma někdy zasažena malwarem nebo jiným malwarem?
- Zažili jste někdy výpadek IT infrastruktury? Jaký byl jeho dopad?
- Máte obavy, jak by výpadek mohl zasáhnout vaše podnikání?
- Jaké škody nastanou každou hodinou mimo provoz?
- Máte plán pro případ nedostupnosti systémů nebo dat?
- Můžete pokračovat v běžném provozu v případě dočasného výpadku? Pokud ano, na jak dlouho?
- Máte kvůli své současné situaci obavy?
- Jakým právním rizikům budete vystaveni, pokud vaše služby budou neočekávaně nedostupné?
- Jak dlouho reálně můžete fungovat bez přístupu ke svým datům?
- Jaký dopad na vaši reputaci by měla situace, kdy celý den nemůžete obsloužit své zákazníky?
- Zkontrolovali jste si své pojištění infrastruktury a dat, a můžete zůstat bez odškodnění, pokud nepoužíváte specifické nebo nejnovější dostupné druhy ochrany?

Obvykle při těchto typech konverzace MSP čelí námitkám od zákazníků týkajících se vyšší ceny pokročilého řešení (jako EDR) a dojmu, že zákazníkův podnik je příliš malý na to, aby byl atraktivním cílem pro útočníky. To však nemůže být dále od pravdy.

Zde jsou některé z nejčastějších námitek, se kterými se MSP setkávají, a jak jim oponovat:

"Už používáme antivirus, nepotřebujeme EDR."

Nadneseně řečeno jde o míchání jablek s hruškami, což samozřejmě zákazník nebere v potaz. Nepočítají nejen s rozdílnou úrovní ochrany, ale podceňují také cenu práce a ztraceného času při řešení a analýze útoků. Je tedy dobré je seznámit nejen s rozdíly v úrovní ochrany, ale také s tím, kolik času je potřeba věnovat správě bezpečnosti v případě každého řešení.

EDR nabízí široké možnosti, které přesahují samotnou ochranu proti virům.
Zde je rychlé porovnání:

AV

- Chrání před viry a malwarem. Typicky k tomu potřebuje pravidelné skenování.
- Obvykle se spoléhá na databázi signatur. To znamená, že výrobce AV musí detekovat škodlivý software a distribuovat aktualizaci svým uživatelům a uživatel samozřejmě musí mít svou databázi aktuální.
- Vyžaduje, aby administrátor prováděl pravidelné skeny a kontrolu.

EDR

- Chrání před více různými vektory hrozeb – včetně bezsouborových útoků, skriptů v dokumentech a škodlivých skriptů spouštěných mimo obvykle skenovaná umístění – pomocí AI se zaměřením na chování jednotlivých procesů, ne pouze databázi známých hrozeb.
- Aktivně vyhledává možné hrozby místo spoléhání na skeny. Pokud narazí na podezřelou aktivitu, upozorní správce v reálném čase (pokud je upozornění potřeba).
- Automatizuje reakce na potenciální hrozby. Některá EDR, jako N-able EDR, umožňují automatizovaný rollback na zařízeních s Windows do posledního bezpečného stavu během vteřin až minut, čímž umožňují zvrátit jakoukoliv způsobenou škodu.

Podle průzkumů[8] a zkušeností našich bezpečnostních expertů je obvyklý čas strávený na nápravě a nastavení prevence poté co antivirus zachytí útok zhruba 3,5 hodiny. Oproti tomu, díky kvalitě analytických dat a telemetrie zaznamenané s EDR v kombinaci s automatizací řešení včetně možnosti rollbacku, lze snížit dobu řešení na cca 5-30 minut.

“Vypadá to příliš nákladně ”

Pokud se zaměříte na hodnotu poskytnutou vašimi službami, nebudete mít problém zmírnit tyto obavy. Pomozte zákazníkovi pochopit, jaké další náklady mohou způsobovat tím, že nepřejdou na komplexnější bezpečnostní řešení.

“Nám se to nemůže stát, jsme příliš malá firma. ”

Každý je se může stát cílem útoku. Zákazník nemusí být hlavním cílem, může sloužit jako gateway pro další útoky nebo součást botnetu. Pomozte jim tedy vyhnout se tomu, aby byli nejslabším článkem.

“Raději to risknu, v případě napadení zaplatím výkupné a budu vyžadovat náhradu od pojišťovny”

Nespoléhejte se pouze na pojišťovnu – budou hledat jakékoliv zanedbání z vaší strany. Nedávejte jim tedy důvod odmítnout vyplatit odškodné.

„Mě se to nemůže stát – kdo by chtěl moje data?”

Možná útočníci nebudou chtít vaše data, ale mohou je zašifrovat a držet jako rukojmí, protože na rozdíl od nich jsou pro vás důležitá a můžete riskovat existenci firmy, pokud o ně přijdete. Potřebují vás dostat do pozice, kdy budete muset zaplatit výkupné.

3 Odhalte reálnou cenu útoku

Vždy, když navrhujete zákazníkům nové bezpečnostní řešení, musíte ho uvést v kontextu, kterému rozumí každé vedení firmy – finančním.

Dvě věci, které rychle opodstatní nákup EDR, jsou cena výpadku, která je způsobena ztracenými obchodními příležitostmi, a čas ztracený návratem do plného provozu, který stojí čas a úsilí zaměstnanců, které by jinak mohlo být využito produktivněji.

Pro upřesnění můžete vedení zákaznické firmy požádat, aby si představili scénář, kdy dojde k napadení a následnému úplnému výpadku jejich systémů. Pak společně spočítejte celkové náklady včetně ztrát na tržbě – v porovnání s tím bude EDR vypadat jako velmi výhodná nabídka.

Cena výpadku může být odhadnuta zhruba takto: Ztracený produktivní čas zaměstnanců + Ztracená tržba + Cena obnovy + Další náklady a potenciální ztráty, které mohou zahrnovat cokoliv z následujícího:

- Platba výkupného za ransomware
- Pokuty za nedodržení předpisů
- Právní náklady
- Vyšší cena pojištění do budoucna
- Konzultace a školení zaměstnanců
- Vedlejší škody
- Ztráta zakázek nebo zákazníků
- Ztráta reputace

Zde je příklad, podle kterého můžete vést konverzaci:

Předpoklady:

Vaším klientem je účetní firma se 40 zaměstnanci, kterou zasáhl ransomwarový útok, který způsobil téměř kompletní výpadek na 24 dní. Při 8 pracovních hodinách za den jde o 192 hodin výpadku produktivní doby.

V ušlé produktivitě za tuto dobu, za předpokladu že budou postiženi všichni zaměstnanci a při výši průměrné mzdy v oboru okolo 240Kč/h, by výpočet mohl vypadat takto:

The EDR ROI best practices and examples shared in this guide were brought to you by N-able's HeadNerd Stefanie Hammond.

Follow the N-able HeadNerd team for more best practices on how to grow your MSP business, security events, and bootcamps.

Cena výpadku (192 hodin) **1.Ztráta produktivního času** **Oddělení postižená výpadkem:**	**Všechna**
Počet zaměstnanců ve firmě	40
Počet zaměstnanců postižených útokem	40
Průměrně ztracených % produktivity	100%
Průměrné náklady na zaměstnance za hodinu	240 Kč
Celkem hodin mimo provoz	192
Ztráta za neproduktivní čas	1 843 200 Kč

Tipy a příklady pro demonstraci EDR ROI sdílené s vámi prostřednictvím tohoto eGuidu pro vás připravila Stefanie Hammond, N-able HeadNerd. Sledujte N-able HeadNerd team pro více nejlepších praktik pro růst vaší MSP firmy, událostí se zaměřením na bezpečnost a bootcampů pro jednotlivá témata.

Na straně ušlého výdělku za konzervativního předpokladu ročního výdělku okolo 2 400 000 Kč, na 240 pracovních dní (5 dní v týdnu x 48 týdnů v roce), a s tím že nebude možné ušlý příjem vynahradit, takto by vypadal výpočet ztráty:

Cena výpadku (192 hodin) **2. Ztráta příjmů**	
Celkový roční obrat	7 200 000 Kč
Počet pracovních dní v roce	240
Počet pracovních hodin denně	8
% příjmu které nelze získat zpět	100%
Ztráty za den	30 000 Kč
Ztráty za hodinu	3 750 Kč
Ztráty za dobu výpadku	720 000 Kč

Další složkou pak jsou náklady na obnovu. Pokud cenu zásahu stanovíme na 1500K4/h, kalkulace bude vypadat takto:

Cena výpadku (192 hodin) **3. Náklady na nápravu**	
Počet hodin do plné obnovy	192
Hodinová sazba za obnovu systémů	1 500 Kč
Celkové náklady na obnovu	288 000 Kč

Celkové ztráty způsobené výpadkem tedy můžeme odhadnout jako součet výdajů za zaměstnance, ušlého zisku za dobu výpadku a nákladů na obnovu:

Celkové ztráty	**2 851 200 Kč**
Celkové ztráty za hodinu	**14 850 Kč**

Pokud pak přidáme možné další škody jak bylo uvedeno výše, celková škoda způsobená útokem může být daleko vyšší. Například průměrná platba za dešifrování je podle průzkumu společnosti Palo Alto 925 000$, ale snadno může přesáhnout i 1 000 000$.

K odhadu celkové škody musí společnost posoudit, jaké další náklady a ztráty jsou relevantní pro jejich společnost podle následujících parametrů:

- Naruší útok schopnost společnosti splnit rozpracovaný projekt?
- Může kvůli delším dodacím lhůtám firma ztratit zákazníky?
- Jak se změní pohled potenciálních zákazníků na vaši firmu?

Jinak řečeno, jaký by taková událost měla dopad na aktivitu, reputaci a následkem toho finance vaší společnosti?

Celkový dopad znamená zbytečně vynaložené náklady na provoz, obnovu a ztrátu části příjmů vlivem zhoršení reputace, odchodu části zákazníků a další nepředvídané škody.

Pokud porovnáme cenu nastíněnou v příkladu výše s cenou EDR řešení, které pomůže odvrátit následky ransomwarového útoku, mohou být úspory ohromující.

4 Navrhněte řešení a plány zabezpečení do budoucna

Vaše celková úroveň zabezpečení je pouze tak silná jako její nejslabší článek. Pokud necháte své zákazníky vytvářet svá bezpečnostní řešení a opatření čistě podle předem navrženého a ničím nepodloženého rozpočtu, útok na zákazníka může být rizikem i pro vás coby MSP.

Best practices jsou následující:

- Vytvořte základní bezpečnostní standard a nasaďte ho jako povinný u všech vašich zákazníků. Se stále se zvyšující úrovní útoků se proaktivní řešení s heuristickou detekcí, jako např. EDR, mohou stát klíčovými při ochraně proti nejnovějším hrozbám – známým i neznámým – a mělo by na ně mělo být nahlíženo jako na součást základní úrovně zabezpečení.
- Předveďte svou bezpečnostní expertízu a plánovací schopnosti vysvětlením jednotlivých součástí bezpečnostního plánu svým zákazníkům a ujistěte se, že je dodržován.

5 Stanovte si podmínky, pokud EDR nepřijmou

Jako MSP/MSSP jste bezpečnostním expertem pro vaše zákazníky. Pokud dojde k nějakému problému, budou volat vám a čekat od vás řešení. Pokud nebudou souhlasit s bezpečnostním programem který jste vytvořili, musí na sebe převzít zodpovědnost za nedodržení vašich doporučení.

V rámci ochrany vaší vlastní firmy pak můžete se zákazníkem vytvořit novou smlouvu o službách s omezením toho, za která rizika nesete zodpovědnost, potvrzení toho že zákazník přijímá riziko a novou sazbu pro řešení výpadků, kde nebyla použita odpovídající úroveň ochrany.

Shrnutí

Demonstrací ROI během procesu vyjednávání se zákazníkem je o představení kontextu a uvedení příkladů. Strategie nastíněné výše by vám měly pomoci být přesvědčivější. Jako další body, které vám pomohou s přesvědčováním, můžete uvést pozitivní hodnocení nebo případové studie zákazníků, kteří již vaše bezpečnostní služby používají, a průzkumy nebo reporty z různých odvětví. Ty mohou předvést, jak vysoké nároky na výkupné obvykle útočníci mají, nebo statistiky množství a škod způsobených útoky, pokud nebudou dostatečně zabezpečeni. Vše, co přinese důkaz o hodnotě nabízeného řešení, pomůže zdůraznit důležitost diskuze a zvýšit důvěryhodnost vaší organizace.

Pokud chcete doporučení z tohoto eGuide plně využít, budete potřebovat skvělé řešení ochrany koncových bodů, které budete nabízet svým zákazníkům.

Zjistěte více

Pro více informací navštivte
https://www.zebra.cz/produkty-n-able/n-able-endpoint-detection-and-response/

Zdroje

[1]https://www.n-able.com/resources/state-of-the-market-the-new-threat-landscape
[2]https://www.n-able.com/press/press-releases/n-able-partners-worldwide-say-goodbye-to-legacy-av-solutions-in-favor-of-sentinelone-edr-to-protect-over-1-million-customer-endpoints
[3] https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-august-2022-97-million-records-breached
[4]https://www.sonicwall.com/2022-cyber-threat-report/
[5]https://www.ibm.com/security/data-breach
[6]State of the Market: The New Threat Landscape. Pushing MSP Security to the Next Level, N able report, March 2022: https://www.n-able.com/resources/state-of-the-market-the-new-threat-landscape
[7]State of the Market: The New Threat Landscape. Pushing MSP Security to the Next Level, N able report, March 2022: https://www.n-able.com/resources/state-of-the-market-the-new-threat-landscape
[8] https://blog.barracuda.com/2019/09/26/threat-spotlight-inefficient-incident-response/#:~:text=Inefficient%20incident%20response%20 %E2%80%94%20Suspicious%20emails,click%20on%20a%20malicious%20link.
[9] Average days of downtime is 24, according to a 2022 Coveware report: https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022
10 https://www.paloaltonetworks.com/blog/2022/06/average-ransomware-payment-update/#:~:text=The%20numbers%20are%20startling%3A%20The,rose%2071%25%20from%20last%20year

O N-able

N-able je již více než 20 let dodavatelem nástrojů pro poskytovatele řízených služeb (MSP), kteří je využívají ke správě, monitoringu a zabezpečení IT infrastruktur svých zákazníků. Řešení N-able využívá přes 22 000 MSP poskytovatelů pro správu více než 500 000 firemních sítí a 7 milionů koncových bodů. Více informací naleznete na n-able.com

O ZEBRA SYSTEMS

Společnost ZEBRA SYSTEMS s.r.o. je s více než 25 lety na trhu předním distributorem s přidanou hodnotou v segmentu IT bezpečnosti a ochrany dat v České republice a na Slovensku. Vedle prodeje produktů poskytuje svým zákazníkům špičkové služby podpory a školení. Společnost je distributorem produktů značky Acronis, GFI Software, Kerio, Exinda, Cloudflare a N-able. Více na www.zebra.cz.

ZEBRA SYSTEMS

ZEBRA SYSTEMS s.r.o.
Tř. SNP 402
500 03 Hradec Králové

Tel: +420 491 615 380
n-able@zebra.cz
www.zebra.cz