Jak nastavit účinnou strategii kybernetické bezpečnosti

Průvodce pro malé a střední firmy

ESET
Digital Security
Progress. Protected.

Ve velkých firmách obvykle existují celá oddělení, která dohlíží na kybernetickou bezpečnost a vytvářejí účinné strategie. Ale co malé a středně velké firmy (SMB) s jen několika interními IT specialisty? Jak by měly postupovat, aby si zajistily odpovídající ochranu, aniž by se zahltily všemožnými opatřeními?

Zde je několik tipů od **Michala Jankecha, viceprezidenta pro segment SMB a MSP ze společnosti ESET.**

ESET®
Digital Security
Progress. Protected.

Kde začít?

Ve většině případů mají malé a střední firmy jen omezený počet pracovníků, kteří se starají o strategii digitálního zabezpečení, pokud vůbec nějaké mají.
Proto je pro ně zásadní zaměřit se na největší hrozby a investovat energii do oblastí, které jsou důležité pro kontinuitu jejich podnikání.

„Měly by přijmout přístup založený na vyhodnocení rizik, který zahrnuje identifikaci nejzásadnějších zranitelností,“ vysvětluje Jankech a dodává, že malé a střední firmy by se měly nejprve zaměřit na následující oblasti.

- **Ochrana dat a šifrování**
- **Vícevrstvá ochrana koncových zařízení a omezení přístupu uživatelů**
- **Vícefázové ověřování (MFA) a pravidelné aktualizace**
- **Kvalitní poskytovatelé e-mailových služeb a vzdělávání zaměstnanců**
- **EDR nebo MDR pro náročné uživatele**

Ochrana dat a šifrování

Jsou všechna vaše zařízení chráněna silným heslem? Výborně. Přesto byste toho měli udělat víc, pokud chcete svá zařízení co nejvíce zabezpečit. **„Všechna koncová zařízení by měla být šifrovaná.“** Představte si, že vám někdo ukradne počítač. Dobře, nemůže se dostat dovnitř, protože nezná heslo a uživatelské jméno, ale přesto se může dostat k datům tím, že vyndá pevný disk. Ujistěte se, že jsou řádně zašifrována nejen přenosná zařízení, ale i stolní počítače," doporučuje Jankech.

„Jednou jsem navštívil zdravotnické zařízení a viděl jsem, že mají hned na recepci počítač, který není zabezpečený heslem. Někdo se mohl snadno vloupat dovnitř, počítač ukrást a získat tak přístup ke všem údajům o pacientech. Takovým scénářům lze předejít zavedením účinných opatření na ochranu dat a šifrováním."

Vícevrstvá ochrana koncových zařízení a omezení přístupu uživatelů

„Zásadní je omezit administrátorské účty. V mnoha případech jsou to lidé, kteří mohou způsobit největší škody. Pokud sabotér získá přístup k účtu administrátora, může do zařízení potenciálně nainstalovat cokoli," říká Jankech.

Uvědomte si také, že jedna vrstva ochrany nestačí. „Je to jako se zabezpečením rodinného domu. V takovém případě byste také použili opatření, která posílí vaši ochranu – bránu, bezpečnostní dveře, alarm a plot. … Mnoho lidí říká, **že doba antivirů je pryč**. Ano, doba standardních antivirových programů, které pracují pouze se signaturami, je už minulostí. Taková řešení už nejsou schopna pokrýt obrovskou škálu současných hrozeb," pokračuje Jankech.

Místo toho se doporučuje **vícevrstvý software pro zabezpečení koncových zařízení,** který je založen na principech strojového učení a který nabízí ochranu podle typu chování, blacklist nebezpečných webových stránek a blokování přístupu k rizikovým doménám, včetně ochrany před síťovými útoky nebo zranitelnostmi v protokolu vzdálené plochy.

Pro malé a střední firmy má smysl investovat nejvíce do prevence. Klíčové je zabezpečení vašich systémů, jejich aktualizace a používání kvalitního softwaru pro ochranu koncových zařízení.

Michal Jankech,
viceprezident pro segment SMB a MSP ve společnosti ESET

„Nejde jen o to, aby byla ochrana zavedena, ale také aby byla správně nakonfigurována a aktualizována," dodává Jankech. Například je třeba se ujistit, že software pro ochranu koncových zařízení nelze odinstalovat, nebo změnit jeho konfiguraci.

Používejte konzoli pro správu koncových zařízení.
„Mnoho společností si myslí, že stačí používat klienta pro ochranu koncových zařízení. Nikdy však nevíte, zda funguje správně, pokud jej nespravujete prostřednictvím konzole, která vám umožní dohlížet na celou síť. I když máte ve firmě jen 10 počítačů, nebudete je moci správně zkontrolovat, zejména v dnešní době, kdy lidé stále častěji pracují z domova a cestují," doporučuje Jankech. Konzole by vám zároveň měla poskytovat přehledy, které můžete kontrolovat, abyste si byli stoprocentně jisti, že jsou vaše systémy a síťový provoz ve správném stavu.

MFA a pravidelné aktualizace

Vícefázové ověřování (MFA) by mělo být zavedeno na všech pracovních i soukromých zařízeních. Udržujte také všechny operační systémy v nejnovějších verzích. „Většina útoků se objevuje v důsledku krádeže identity a hesla nebo díky zneužití obecně známé zranitelnosti v operačním systému," vysvětluje Jankech.

S každou novou verzí operačního systému výrobce opravuje případné nedostatky a zmenšuje se tak šance, že kyberzločinci najdou cestu do firemních zařízení. **Doporučují se automatické aktualizace.** „Pokud jde o malé a střední firmy, zero-day útoky se objevují jen výjimečně. Pokud používáte vlastní software, je pravděpodobnost, že kyberzločinci provedou takový útok, poměrně malá. Ve většině případů jsou dveřmi, kterými útočníci pronikají do vaší firmy, známé zranitelnosti v běžně používaném nebo open-source softwaru," říká Jankech.

> **Lékaři, architekti, PR agentury... ti všichni potřebují strategii kybernetické bezpečnosti. Mnoho lidí si například neuvědomuje, že některé dokumenty jsou chráněny autorským právem, a proto by měly být odpovídajícím způsobem chráněny.**
>
> **Michal Jankech**,
> VP of the SMB & MSP segment at ESET

Kvalitní poskytovatelé e-mailových služeb a vzdělávání zaměstnanců

Klíčem jsou také spolehliví poskytovatelé e-mailových služeb. „Zaměstnanci by také měli vědět, jak odhalit phishingový e-mail. Příjemcům e-mailů také můžete dát vědět, že zpráva přišla zvenčí. Office 365 umožňuje označit e-maily štítkem ‚externí'," doporučuje Jankech. Čas od času se vyplatí investovat do školení zaměstnanců v oblasti kybernetické bezpečnosti, aby se zvýšila jejich informovanost. **Několik tipů, jak udělat vzdělávání efektivní a zábavné** můžete získat na stránkách ESET Digital Security Guide.

Jankech zdůrazňuje, že většina společností nemá tato základní opatření zavedena a někdy jsou v digitálním zabezpečení velkých podniků dokonce ještě větší mezery. „Některé společnosti stále váhají s investicemi do kybernetické bezpečnosti nebo si myslí, že se nestanou terčem útoku, protože oblast jejich podnikání není pro útočníky atraktivní. Kybernetické útoky však obvykle nejsou cílené. Obětí se může stát kdokoli," upozorňuje odborník na kybernetickou bezpečnost.

EDR nebo MDR pro pokročilé uživatele

Jakmile máte všechny základní prvky kybernetické bezpečnosti pevně zavedeny, je na čase začít používat **pokročilé nástroje kybernetické bezpečnosti jako je například komplexní detekce a ochrana koncových zařízení (EDR).** „Jde o zcela nový segment trhu, který je postaven na předpokladu, že prevence vždy selhává. Toto řešení používají převážně velké firmy, které si mohou dovolit luxus mnoha interních IT oddělení a vlastní bezpečnostní operační centrum (SOC, Security Operations Center) s nepřetržitým provozem. Dodržování tohoto přístupu obvykle vede k přijetí postoje, že kyberzločincům se nakonec může podařit napadnout váš systém," dodává Jankech.

Řešení EDR identifikují anomálie a podezřelé chování v síti a v ideálním případě umožňují reagovat zablokováním procesu nebo podle vlastních automatizovaných systémových pravidel. „Ačkoli se tato řešení obvykle používají ve větších společnostech, mohou být přínosem i pro menší firmy.

Základní stavební prvky strategie kybernetické bezpečnosti pro malé a střední firmy

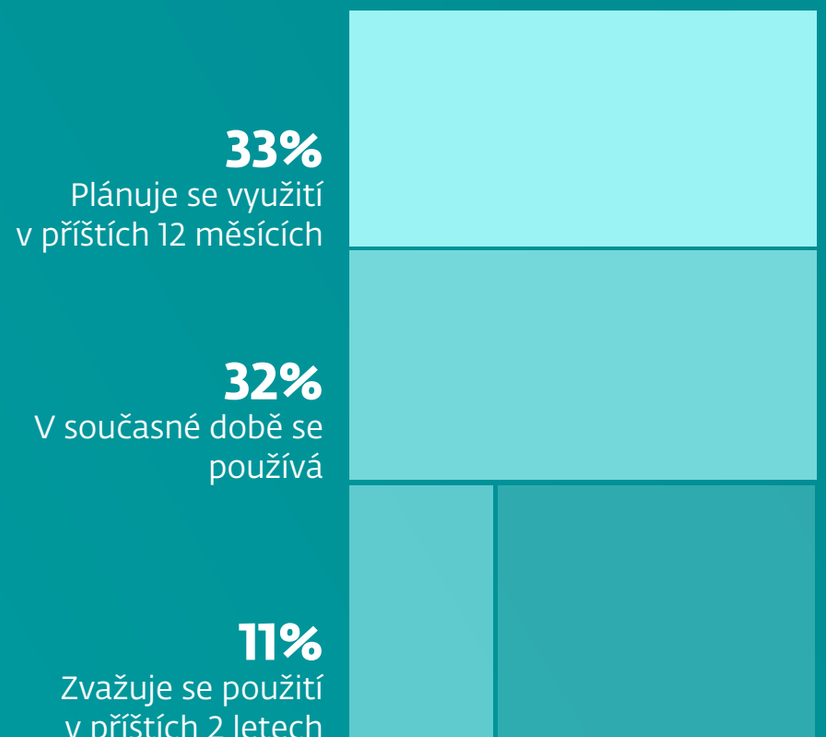
- **Chráněná a šifrovaná data**
- **Pravidla omezeného přístupu pro uživatele**
- **Vícevrstvé zabezpečení koncových zařízení**
- **MFA a aktualizace operačního systému**

Ke správě platformy EDR potřebujete zaměstnance, proto doporučujeme menším firmám, které mají možnost EDR využít, aby se poohlédly po outsourcingu těchto služeb," dodává Jankech.

A právě v těchto případech se nabízí MDR (Managed Detection and Response). MDR je vlastně EDR, které je řízené třetí stranou. „Z jednoho monitorovacího centra jsou pod dohledem desítky nebo dokonce stovky zákazníků a obvykle je k dispozici i nepřetržitá infolinka, na kterou se můžete obrátit," říká Jankech.

Nicméně o EDR nebo MDR byste měli uvažovat pouze v případě, že již máte zajištěny základní funkce. Používáním EDR nebo MDR zvyšujete šanci, že vaše firma odolá kybernetickým útokům a bude v bezpečí, zároveň je ale potřeba být stále ve střehu.

Používání řešení EDR / XDR / MDR



Source: 2022 ESET SMB Digital Security Sentiment Report

O SPOLEČNOSTI ESET

Společnost ESET® již více než 30 let vyvíjí špičkový software a služby v oblasti IT bezpečnosti, které chrání firmy, kritickou infrastrukturu a spotřebitele po celém světě před stále sofistikovanějšími digitálními hrozbami. Vysoce výkonná a snadno použitelná řešení společnosti ESET, od zabezpečení koncových zařízení a mobilních zařízení přes pokročilou detekci na koncových zařízeních až po šifrování a vícefázovou autentizaci, chrání a monitorují 24 hodin denně, 7 dní v týdnu a aktualizují ochranu v reálném čase, aby uživatelé byli v bezpečí a firmy fungovaly bez přerušení. Vyvíjející se hrozby vyžadují vyvíjející se IT bezpečnostní společnost, která umožňuje bezpečné používání technologií. Za tím stojí výzkumná a vývojová centra společnosti ESET po celém světě, která pracují na naší společné budoucnosti. Pro více informací navštivte www.eset.com nebo nás sledujte na LinkedIn, Facebooku a Twitteru.

Digital Security
Progress. Protected.