Průvodce odbornou terminologií

www.sharp.cz

SHARP
Be Original.

Složité bezpečnostní pojmy, zjednodušeně

Kybernetická kriminalita může pro digitálně propojené firmy nabývat mnoha podob. Pochopení, jak může útok vypadat, jak se může projevit a jaké může mít důsledky pro vaše podnikání, by nemělo být podceňováno.

Pro mnohé malé a střední podniky (MSP) však není řešení této hrozby prvořadou prioritou. Aby bylo možné se účinně bránit kybernetickým hrozbám, je nutné skutečně porozumět významu všech těchto odborných termínů.

Pro lepší pochopení jsme pro vás rozklíčovali některé z nich.

Zabezpečení sítě

Pevný zámek chránící vaše informace

Podobně jako zamykáte své cennosti do trezoru nebo připoutáváte kolo k zdi, síťová bezpečnost chrání citlivé informace vaší firmy.
Toto ochranné opatření je nezbytné pro každou firemní síť. Vaše bezpečnostní opatření by mělo zahrnovat systém pro detekci narušení (IDS), který je navržen k sledování a identifikaci potenciálních hrozeb, podezřelých aktivit a neoprávněných pokusů o přístup na digitálně propojená zařízení, jako jsou notebooky a tiskárny.

Porušení ochrany dat

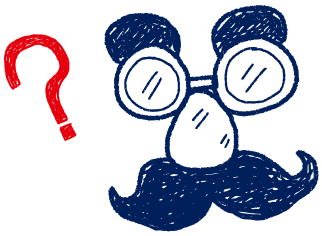
Jako když vám někdo ukradne peněženku ve vlaku

Nemusíte si hned uvědomit, že se to stalo, až do doby kdy se vaše data dostanou do nesprávných rukou. Porušení ochrany dat nastává, když citlivé informace - ať už patří firmě nebo klientovi - jsou odcizeny kyberzločinci. K tomu může dojít, aniž by si toho firma byla vědoma. Porušení ochrany dat může vést k ztrátě důvěry zákazníků nebo uživatelů, poškození pověsti značky a dokonce i k vysokým pokutám ze strany regulačních orgánů.

Phishing, smishing a vishing

Jednoduše řečeno: hacker převlečený za vašeho šéfa, klienta, nejlepšího přítele nebo oblíbený obchod s oblečením

Tyto typy útoků nemusí být na první pohled zřejmé, ale jsou velmi běžné. Ve skutečnosti začíná asi 90% kybernetických útoků phishingem (e-mail), zatímco počet útoků smishing (SMS) a vishing (telefonní hovor) také stoupá. Všichni jsme již viděli podezřelé e-maily ve složce se spamem. Phishing, smishing a vishing jsou kybernetické útoky, které klamou uživatele, aby klikli na e-maily, reagovali na zprávy nebo odpovídali na hovory, o kterých si myslí, že jsou legitimní. Pokud je útok úspěšný, zaměstnanci jsou pak bez jejich vědomí oklamáni k poskytnutí citlivých informací, jako je heslo k síti.



Malware

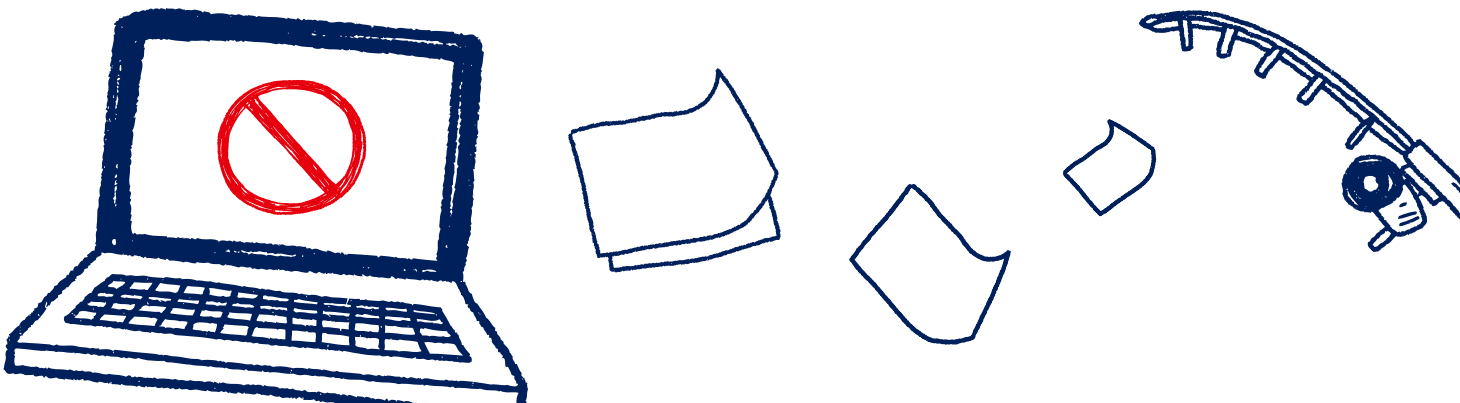
Škodlivý druh softwaru, vytvořený čistě se zlými úmysly

„Malware“ je zkratka pro škodlivý software. Jedná se o software navržený kyberzločinci s cílem poškodit síťové systémy vaší firmy a zabránit vám v jejich používání. Malware může infiltrovat váš systém v důsledku otevření phishingového e-mailu, kliknutí na podezřelý odkaz nebo návštěvy již kompromitované webové stránky. Jakmile se to stane, informace uložené ve vaší síti mohou být vystaveny hackerům, což vede k eskalaci útoku.

Ransomware

Vaše data jako rukojmí

Ransomware, forma škodlivého softwaru, je používán kyberzločinci k zablokování přístupu k zásadním obchodním informacím zašifrováním (přeměnou dat na kód). Každý digitálně propojený podnik vlastní data, od finančních záznamů po výsledky testů pacientů a důvěrné právní dokumenty. Přístup k těmto datům je nezbytný pro chod podniku. Nicméně, jakmile ransomware infikuje vaši síť, může váš podnik tento přístup ztratit. Aby bylo možné jej znovu získat, často je nutné zaplatit výkupné (velice vysoké sumy) hackerovi, který útok provedl.



Zabezpečení koncových zařízení

Zajištění, že všechna vaše zařízení jsou stejně bezpečná jako vaše PC

Vaše digitální ocharna nezačíná a nekončí pouze u stolního počítače. Zabezpečení koncových zařízení znamená proces zajištění ochrany všech vašich „koncových zařízení“; od tabletů a smartphonů po další připojená zařízení k internetu (jako je tiskárna ve vaší kanceláři), aby měla společnou ochranu. Tato ochrana by měla být centrálně spravována a monitorována, aby bylo možné získat reálný pohled na vaši pozici v oblasti kybernetické bezpečnosti.

Správa aktualizací

Představte si: aktualizace vašeho telefonu na nejnovější operační systém

Většina z nás se pravděpodobně setkala s těmito softwarovými aktualizacemi na našich PC nebo telefonech: „aktualizujte nyní Windows 10“ nebo „instalujte iOS 9.999“. Tyto aktualizace jsou však klíčovým bezpečnostním opatřením. Správa aktualizací je proces aplikování aktualizací na software, ovladače a firmware za účelem ochrany síťových zranitelností. Zahrnuje dohled nad dodržováním předpisů, správu aplikací, které vaše firma používá, a zajištění, aby vaše systémy fungovaly na plný výkon.

Zůstaňte v bezpečí

Ačkoli je to složité, porozumění odbornému jazyku kybernetické bezpečnosti je dnes důležité pro každý digitálně propojený podnik.

Zároveň společnost Sharp nabízí širokou škálu specializovaných služeb a řešení v oblasti kybernetické bezpečnosti, díky čemuž je pro vás snazší zvládat rizika.

Centrum Sharp Real World Security

Šifrování

Představte si všechna vaše data, zamíchaná jako písmena ve Scrabble sáčku.

Jak zabránit někomu ve čtení tajné zprávy? Zamícháte slova, písmena a čísla. To je v podstatě to, co dělá šifrování. Šifrování převádí “čitelný text” – vaše citlivá data – do “šifrovaného textu”, což z něj činí nesrozumitelný obsah pro každého, kdo nemá “dekódovací klíč”, tedy heslo, které používáte například pro přístup k zabezpečené bezdrátové síti. Ve firmě by mělo být šifrování aplikováno na všechna zařízení, jako jsou telefony a notebooky, aby obsah uložený v každém zařízení nebyl čitelný, pokud je zařízení ztraceno nebo ukradeno.

Reakce na incidenty

Váš akční plán pro odražení útoku

Co je prvním krokem, když je vaše firma ohrožena kybernetickým útokem? Reakce na incidenty (IR) je systematický postup, který organizace používají, aby plánovaly, jak efektivně reagovat a zvládat kybernetické bezpečnostní incidenty. Pokud nemáte pro takové situace připravený pevný plán IR, může to vaší firmě zabránit v účinné obraně – a ta je klíčová pro zachování integrity, důvěrnosti a dostupnosti citlivých obchodních dat.