Základy síťové bezpečnosti pro malé podniky

Co je to síťová bezpečnost?

Síťová bezpečnost je jakákoli činnost, jejímž účelem je zachovávat použitelnost a integritu sítě a dat. Zahrnuje hardwarové i softwarové technologie. Efektivní zabezpečení sítě řídí i přístup do ní. Cílí na široké spektrum hrozeb a blokuje jejich průnik nebo šíření v síti.

Jak zabezpečení sítě funguje?

Síťová bezpečnost kombinuje několik vrstev obrany na okraji a uvnitř sítě. Každá vrstva síťové bezpečnosti uplatňuje pravidla a provádí kontrolu. Oprávnění uživatelé získávají přístup k síťovým zdrojům, ale škodlivé entity a bezpečnostní hrozby jsou blokovány.

Jaký mám ze síťové bezpečnosti užitek?

Digitalizace mění náš svět. Způsob, jakým žijeme, pracujeme, učíme se a hrajeme si, se zcela změnil. Všechny podniky a organizace, které chtějí poskytovat služby, jaké jejich zákazníci a zaměstnanci požadují, musí chránit své sítě. Síťová bezpečnost také pomáhá chránit důvěrné informace před zneužitím a chrání také vaši reputaci.

6 kroků, jak zabezpečit síť

1. Monitorujte příchozí a odchozí datový provoz na svém firewallu a pozorně studujte protokoly. Nespoléhejte na to, že vás na nežádoucí aktivitu upozorní výstraha. Zajistěte, aby někdo ve vašem týmu údajům rozuměl a dokázal patřičně zasáhnout.
2. Sledujte dostupné informace o nově odhalených hrozbách. Například stránka TrendWatch provozovaná společností Trend Micro sleduje aktuální aktivitu bezpečnostních hrozeb.
3. Povolte pravidelné aktualizace firewallu a antivirového softwaru.
4. Provádějte pravidelné školení zaměstnanců, aby rozuměli všem změnám ve vaší politice přijatelného užívání zdrojů. Podporujte také přístup k bezpečnosti na principu „sousedských hlídek“. Všimne-li si zaměstnanec čehokoli podezřelého, například že se mu nedaří přihlásit ke svému emailovému účtu, měl by okamžitě uvědomit příslušnou osobu.
5. Nainstalujte řešení na ochranu dat. Tento druh zařízení dokáže ochránit váš podnik před ztrátou dat, dojde-li k narušení bezpečnosti sítě.
6. Zvažte zavedení dodatečných bezpečnostních řešení, která zvýší úroveň ochrany vaší sítě a rozšíří schopnosti vašeho podniku.

Základy síťové bezpečnosti pro malé podniky

Typy řešení pro síťovou bezpečnost

Řízení přístupu

Ne každý uživatel by měl mít přístup do vaší sítě. Abyste dokázali zabránit možným útočníkům v průniku, musíte rozpoznat každého uživatele a každé zařízení. Poté můžete uplatňovat bezpečnostní pravidla. Můžete blokovat koncová zařízení, která nesplňují kritéria nebo jim poskytnout pouze omezený přístup. Tento proces se nazývá řízení přístupu k síti (NAC).

Software na ochranu proti virům a malwaru

Pojmem „malware“ se označuje souhrnně škodlivý software včetně virů, červů, trojských koní, vyděračského softwaru a špionážního softwaru. V některých případech malware pronikne do sítě, ale zůstane po řadu dní nebo i týdnů nečinný. Nejlepší antimalwarové programy nejen vyhledávají malware na vstupu, ale i poté nepřetržitě sledují soubory a detekují anomálie, odstraňují nalezený malware a napravují škody.

Bezpečnost aplikací

Každý software, který váš podnik užívá při svém provozu, potřebuje ochranu, bez ohledu na to, zda byl vyvinut interně nebo zakoupen. Každá aplikace může obsahovat zranitelnost, které mohou útočníci zneužít k průniku do vaší sítě. Bezpečnost aplikací zahrnuje hardware, software a procesy k ošetření zranitelností.

Behaviorální analýza

Aby bylo možné detekovat abnormální chování, musíme nejprve vědět, jak vypadá chování standardní. Nástroje pro behaviorální analýzu automaticky rozpoznávají aktivity vybočující z normy. Váš bezpečnostní tým může snáze odhalit známky narušení bezpečnosti, které ukazují na možný problém, a přijmout příslušná opatření.

Prevence ztráty dat

Podniky a organizace musí zajistit, aby jejich zaměstnanci neodesílali citlivé informace mimo interní síť. Technologie pro prevenci ztráty dat (DLP) dokážou zabránit nahrávání, přeposlání a dokonce i tisku důležitých firemních informací.

Emailová bezpečnost

Emailové brány jsou nejobvyklejší cestou, kterou se útočníci snaží proniknout do sítě. Ti s pomocí osobních údajů a metod sociálního inženýrství vytváří propracované kampaně, které mají oklamat příjemce a nasměrovat je na internetové stránky se škodlivým obsahem. Aplikace zajišťující emailovou bezpečnost blokují útoky zvenčí a kontrolují odchozí zprávy jako prevenci úniku citlivých dat.

Firewally

Firewally staví bariéru mezi důvěryhodnou interní síť a nedůvěryhodné vnější sítě, jako je internet. Povolují nebo blokují provoz na základě nastaveného souboru pravidel. Firewall může být hardwarový, softwarový nebo kombinovaný. Společnost Cisco nabízí zařízení pro jednotné řízení hrozeb (UTM) a firewally příští generace zaměřené na hrozby.

Systémy pro prevenci průniku

Systém pro prevenci průniku (IPS) kontroluje síťový provoz a aktivně blokuje hrozby. Zařízení Cisco Next-Generation IPS (NGIPS) to provádí porovnáváním datového provozu s ohromným objemem globálních poznatků o hrozbách a nejen blokuje škodlivou aktivitu, ale také sleduje pohyb podezřelých souborů a malwaru v síti a brání šíření nákazy.

Základy síťové bezpečnosti pro malé podniky

Bezpečnost mobilních zařízení

Kyberzločinci stále častěji cílí na mobilní zařízení a aplikace. Během příštích 3 let můžeme dospět do situace, kdy IT oddělení 90 % podniků bude podporovat provoz podnikových aplikací na soukromých mobilních zařízeních. Samozřejmě je nutné si zachovat kontrolu nad tím, která zařízení budou mít přístup k síti. Stejně tak je nezbytné mít možnost nastavit jejich připojení, aby zůstal datový provoz důvěrný.

Segmentace sítě

Softwarově definovaná segmentace sítě rozděluje datový provoz do různých kategorií a usnadňuje uplatňování bezpečnostních pravidel. V ideálním případě je klasifikace založená na identitě koncového bodu, nikoli pouhé IP adrese. Přístupová práva lze přidělit podle role, umístění a dalších atributů, aby správní lidé měli správná oprávnění a podezřelá zařízení byla izolována a uvedena do řádného stavu.

Virtuální soukromá síť (VPN)

Virtuální soukromá síť šifruje připojení mezi koncovým bodem a sítí, které často probíhá přes internet. VPN pro vzdálený přístup typicky využívá zabezpečení IPSec nebo Secure Sockets Layer (SSL) k autentizaci komunikace mezi zařízením a sítí.

Webová bezpečnost

Řešení pro webovou bezpečnost hlídá pohyb zaměstnanců po internetu, blokuje internetové hrozby a brání přístupu ke škodlivým stránkám. Chrání vaši internetovou bránu buď lokálně, nebo v cloudu. „Webová bezpečnost“ také zahrnuje opatření na ochranu vašich vlastních internetových stránek.

Zabezpečení bezdrátových sítí

Bezdrátové sítě nejsou tak bezpečné jako pevné sítě. Bez přísných bezpečnostních opatření je zavedení bezdrátové LAN, jako kdybyste rozmístili ethernetové porty po celé firmě, včetně parkoviště. Abyste předešli narušení bezpečnosti, potřebujete produkty určené specificky k ochraně bezdrátových sítí.

Centrála pro Severní a Jižní Ameriku
Cisco Systems, Inc.
San Jose, CA

Centrála pro Asii a pacifickou oblast
Cisco Systems (USA) Pte. Ltd.
Singapore

Centrála pro Evropu
Cisco Systems International
BV Amsterdam, Holandsko

Cisco má více než 200 poboček na celém světě. Adresy, telefonní čísla a faxová čísla jsou uvedená na internetových stránkách Cisco **www.cisco.com/go/offices.**