Quantcom Propojujeme profesionály

Zabezpečte se před zneužitím Vaší ústředny!

Vážený zákazníku, prosíme věnujte zvýšenou pozornost následujícím informacím.

Jelikož narůstá hrozba a množí se případy zneužití zákaznických VoIP systémů (VoIP servery, VoIP PBX, SIP servery, SIP PBX, ...), dovolili jsme si shrnout následující obecná doporučení a základní bezpečnostní zásady. Vzhledem k rozmanitosti problematiky ale nemůžeme garantovat úplnost všech informací. Odbornou implementaci uvedených zásad, která je závislá na konkrétním typu vašeho VoIP systému, si budete muset zajistit sami pomocí vlastních prostředků a na své vlastní náklady.

Dovolujeme si Vás upozornit, že odpovědnost za zabezpečení Vaší VoIP technologie i nadále zůstává jen na Vás.

Zabezpečení VoIP systémů rozhodně není jednoduchou záležitostí a vyžaduje trvalou pozornost a soustavnou činnost. Následující doporučení obsahují jednak běžné bezpečnostní úkony, které jsou zvládnutelné běžným uživatelem, tak i úkony, které vyžadují odborný a profesionální zásah. Tyto úkony bude potřebné svěřit do rukou vašemu správci systému, servisní firmě či dodavateli vašeho systému.

Autentifikační hesla

Používejte bezpečnostně silná autentifikační hesla a to jak pro veškeré administrátorské či uživatelské přístupy do vašeho systému, tak i pro autentifikaci VoIP zařízení (VoIP telefonů) vůči vašemu systému.

- Pro hesla používejte minimálně 8 znaků
- Používejte kombinace písmen (malých, velkých), číslic a nealfanumerických znaků (tečky, čárky, středníky, ...)
- V žádném případě nepoužívejte jména postav z oblíbených seriálů, filmů, večerníčků či počítačových her: Harry Potter, Gandalf, Bob Builder (Bořek Stavitel), Lightning McQueen (Blesk McQueen), Spiderman, Pat a Mat a další. Tato jména bývají velmi často používána k takzvaným Slovníkovým útokům, což je jedna z metod pro odhalení přístupového hesla.

Firewall (bezpečnostní brána) systému

Aktivně využívejte Firewall (bezpečnostní bránu) Vašeho systému, ať už externí firewally (speciální zařízení k těmto účelům zkonstruovaná) či interní firewally (součást operačního systému - typicky Linuxové, FreeBSD či ostatní Unixové distribuce):

- Zamezte všem neoprávněným a neodůvodněným spojením do Vašeho systému.
- Povolte pouze ta spojení, která jsou bezpodmínečně nutná pro funkci systému, jeho služeb a aplikací. Zvažte opravdovou nutnost těchto spojení a zvažte vyplývající bezpečnostní rizika. Snažte se tato spojení v maximální možné míře redukovat. Pravidelně vyhodnocujte jejich oprávněnost.
- Tyto zásady se týkají i všech VoIP zařízení (VoIP telefony, brány, SW klienti na počítačích, další připojené PBX). Globálně zamezte přístup pro všechna VoIP zařízení a explicitně povolte pouze ta, která mají oprávnění volat prostřednictvím vašeho VoIP systému.

Síťové protokoly

- Povolte pouze ty síťové protokoly, které jsou bezpodmínečně nutné pro funkci vašeho systému (typicky pouze IPv4). Deaktivujte všechny protokoly, které používány nejsou.
- Pozor například na protokol IPv6 - pokud není používán aplikacemi, deaktivujte ho.

Systémové služby

Povolte pouze ty systémové služby, které jsou nezbytně nutné pro provoz požadovaných aplikací a zvažte bezpečnostní rizika jejich používání.

- Zvažte použití internetového super serveru "inetd"
- Zakažte FTP, TFTP, TELNET, SSH, ... a další relace, pokud nejsou používané. Pokud existuje odůvodněná potřeba k jejich zavedení, přístup k nim povolte pouze pro explicitně definované počítače (host IP) a porty (pomocí konfigurace služby či firewallu).
- Zabezpečte přístup k databázím. Zcela eliminujte možnost vzdáleného přístupu do databází, případně ho povolte pouze pro explicitně definované počítače a porty.

Hlasové služby

Povolte volání výhradně od autentifikovaných VoIP klientů (VoIP telefony hardwarové, softwarové, VoIP brány, připojené VoIP ústředny atd.).

- Týká se nekompromisně všech VoIP účtů, prostřednictvím kterých může být uskutečněno volání do veřejné telekomunikační sítě. Všechny tyto VoIP účty musí bezpodmínečně vyžadovat autentifikaci od svých VoIP klientů.
- Bezodkladně a s trvalou platností zamezte volání prostřednictvím jakýchkoliv implicitních či defaultních SIP účtů.
- Umožněte volání pouze pro explicitně definované kontexty volání (viz. například Asterisk context). Zamezte volání prostřednictvím implicitních či defaultních kontextů. Logujte pokusy o volání uskutečněné prostřednictvím těchto implicitních kontextů.

Sledování záznamů o uskutečněných voláních

Soustavně sledujte a vyhodnocujte záznamy o uskutečněných voláních (CDR záznamy). Konfrontujte tyto záznamy s realitou. Vyhledávajte zejména volání do podezřelých lokalit (Afrika, Střední a Jižní Amerika, Asie, Ostrovy v Tichomoří a Atlantiku a další). Pokud je to možné, zahrňte do sledování i neuskutečněná volání, tzn. nezdařené pokusy o volání.

Protokolování podezřelých aktivit

Pořizujte a vyhodnocujte záznamy o všech podezřelých aktivitách na Vašem VoIP systému. Myšleny jsou zejména:

- Pokusy o neoprávněnou autentifikaci a přístup do Vašeho VoIP systému.
- Pokusy o neoprávněná či neautentifikovaná volání.
- Přístupy prostřednictvím otevřených služeb (FTP, TFTP, SSH, ... a další)
- Záznamy z Firewallu Vašeho systému.

Obecné zásady

Kombinujte výše uvedené metody a techniky zabezpečení.

Pozorně sledujte problematiku zabezpečení, zejména informace specifické pro Váš VoIP server, a to jak na úrovni provozovaných aplikací, tak i na úrovni operačního systému.

Všechny počítače, které mají vzdálený přístup k vašemu VoIP serveru, musí být samy o sobě velmi dobře zabezpečeny. Jinak hrozí, že se tyto počítače samy stanou prostředníkem k bezpečnostnímu průlomu do vašeho VoIP systému.

S přátelským pozdravem

Technický tým Quantcomu