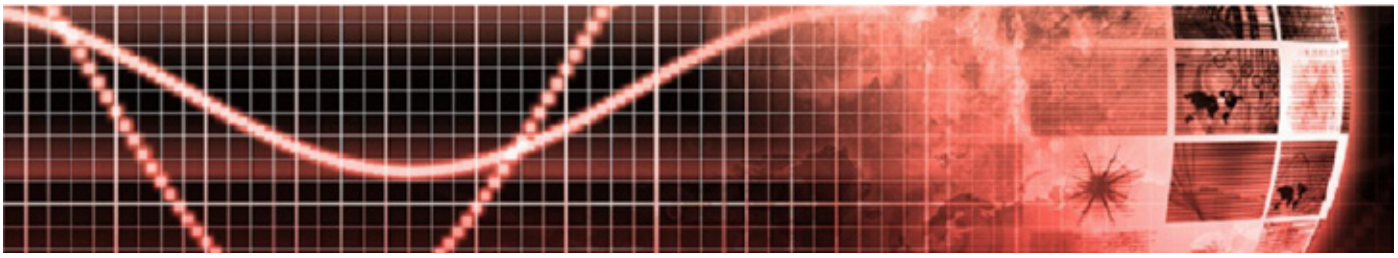
DEEP SECURE



Chat Guard

Chat je pro firmy důležitým nástrojem spolupráce a bývá využíván jak interně, tak ke komunikaci s externími partnery, stále častěji ale i přímo se zákazníky. Zároveň však představuje další kanál, kterým mohou pronikat kybernetické hrozby a může být zneužit.

- Blokace šíření malwaru
- Prevence úniku dat
- Zastavení útoků, které využívají sociální inženýrství
- Obrana proti neznámým hrozbám
- Sledovatelnost uživatelů
- Pokročilé ověřování obsahu
- Sebeobrana

Nástroj Deep-Secure Chat Guard řídí využití standardního internetového chatu a umožňuje vaší organizaci používat jej, aniž by ohrožovala citlivé údaje a důležité firemní postupy.

Tento nástroj využívají firmy, které potřebují mít kontrolu nad externím chatovým provozem nebo chatem mezi oddělenými interními zónami. Může jít například o organizace ze státní správy, právní sféry, obrany, farmaceutického průmyslu, finančnictví nebo komunálních služeb.

Chat Guard ukončuje síťová spojení a získává z nich příslušné XML požadavky a odpovědi na ně. Ověří, zda je jejich obsah přípustný, a teprve poté naváže nové spojení a data doručí. Funguje tedy jako proxy v aplikační vrstvě. Pro útočníka díky tomu nejsou přístupná žádná zranitelná místa ve vnitřní síti. To chrání systém před novými a neznámými útoky a způsoby úniku informací.

Chat Guard také nabízí funkce firewallu a ověřování koncového bodu, obsažené zpravidla ve firewallech nové generace. Dokáže

Bezpečný chat

Chat Guard kontroluje standardní internetový provoz chatu XMPP mezi dvěma servery v různých sítích. Přenášené chatové zprávy transformuje, čímž z nich odstraňuje nežádoucí data a potenciálně nebezpečné konstrukce. Tím chrání proti útokům v podobě pečlivě připravených zlovolných zpráv, které mají zneužít zranitelná místa, a znemožňuje útočníkovi ukrývat informace do jinak legitimních zpráv.

Této transformaci se říká překládka (transshipment). Úseky XML představující jednotlivé chatové zprávy jsou pro účely kontroly transformovány do vlastního pomocného datového formátu Deep Secure, zvaného XDS. Ten je jednodušší než XML, a samotný nástroj Chat Guard se tak nemůže stát obětí zranitelných míst v kódu zpracování XML.

Překládka se nesnaží útoky odhalit. Namísto toho veškerý malware a řídicí data zahodí, protože z chatové zprávy vezme jen užitečné obchodní informace. Chat Guard se tedy nespoléhá na signatury ani detekci anomálií a vždy vás ochrání i proti neznámým hrozbám. Další informace o překládce naleznete v samostatném letáku.

Chat Guard brání odhalení uživatelů a chatových místností. Interní aktivita tedy není viditelná pro externí uživatele. Dále jsou blokovány veškeré formy sdílení souborů, aby nemohl pronikat malware dovnitř ani citlivé informace ven.

Bohatý chat

Ačkoli je komunikace prostřednictvím nástroje Chat Guard důkladně zabezpečená, dojem uživatelů to nenarušuje. Nástroj zpracovává i zprávy ve formátu rich text, takže je zachováno formátování. Jsou přenášeny i informace o stavu uživatelů, takže je vidět, zda jsou přátelé online. Je podporován také chat více uživatelů, takže je možné pořádat společné diskuse v chatových místnostech.

Sebeobrana

Chat Guard je interně rozdělen na zóny, takže relativně složitý kód pro práci s XML je oddělený od z hlediska bezpečnosti kritického kódu pro ověřování obsahu. Díky tomuto rozdělení je prostor pro napadení nástroje Chat Guard velmi malý. Zároveň lze díky využití technologie Ring Architecture (požádáno o patentovou ochranu) od společnosti Deep-Secure tento nástroj spravovat z jediného místa, aniž by došlo k narušení oddělení zón. Výsledkem je Chat Guard schopný sebeobrany, který dokáže odolat i přímému sofistikovanému útoku.

Snadná správa

Ke správě nástroje Chat Guard používají administrátoři webové rozhraní. Provoz lze spravovat pomocí samostatného síťového rozhraní. Správci se mohou identifikovat digitálními certifikáty, což zajišťuje maximální ochranu proti pokročilým útokům.

Chat Guard pomocí standardních protokolů poskytuje záznamy o své činnosti, takže jej lze integrovat do firemního režimu bezpečnosti a správy sítě. Tyto záznamy obsahují informace o provozu XML, který prochází přes Chat Guard, takže monitorovací systém může korelovat aktivitu v celém systému. Dále mohou být obsaženy i záznamy o aktivitách správce, kteří tak mohou být za své činy odpovědní.

Protokoly

Chat Guard podporuje optimalizovaný meziserverový protokol XMPP. Zpravidla se používá spolu s chatovými servery Isode M-Link.

Monitorovací informace lze zasílat firemnímu systému SIEM prostřednictvím protokolů SNMP nebo syslog.

Platformy

Chat Guard se dodává jako zařízení s operačním systémem Deep-Secure DSOS. Tento systém obsahuje pouze funkce nezbytné k fungování nástroje Chat Guard, a prostor k jeho napadení je tedy minimální. Podporuje celou řadu hardwarových platforem.

Deep-Secure LRB je server poloviční výšky 1U do 19” racku. Vnitřní zónování zajišťuje pomocí kernelových mechanismů. Tři síťová rozhraní umožňují samostatné připojení k managementové síti.

Chat Guard lze dodat i jako obraz virtuálního stroje VMWare ESXi. Případně jako sadu tří virtuálních strojů, přičemž virtualizace v tomto případě posiluje vnitřní rozdělení na zóny.

Ke správě nástroje Chat Guard lze použít jakýkoli prohlížeč kompatibilní s HTML5.

Chcete se dozvědět víc?

www.freedivision.com

+420 220 972 426

FREEDIVISION
for safety reasons

April 2014

37Q13321