DYNAMICKÝ MARKETING: PRINCIPY FUNGOVÁNÍ A BEZPEČNOST

DIGITAL SIGNAGES: PRINCIPALS OF FUNCTIONING AND SECURITY

Zdeněk Freund – Jan Lánský

ABSTRAKT
Předkládaný příspěvek se zaměřuje na definici Dynamického marketingu, kde stanovuje jeho rozdělení podle místa využití a způsobu zapojení. Velice důležitou součástí je bezpečnost. V příspěvku se poukazuje na potencionální rizika vyplývající z používání Dynamického marketingu. Tyto potencionální rizika jsou rozděleny do kategorií podle způsobu zapojení či místa použití, dále jsou předkládány důležité základní bezpečnostní řešení, které by měly být při používání Dynamického marketingu zakomponovány, a jsou nastíněny potencionální škody vyplývající ze špatného zabezpečení.

KĽÚČOVÉ SLOVÁ
Dynamický marketing, IPTV, bezpečnost, DoS.

ABSTRACT
The presented article focuses on the definition of digital signage. It states the division according to the place or the way of its plugging. A very important part is the security. The article points out the potentional risks ensuing from the usage of the digital signage. These potential risks are devided into categories according to the way of plugging or the place of usage. Further there are presented important basic security solutions that should be implemented during the usage of the digital signage and also there are mentioned potentional damages ensuing from an insufficient protection.

KEY WORDS
Digital signages, IPTV, Security, DoS.

Dynamický marketing

Dynamický marketing (Digital Signages, Digitalní marketing) by se dal definovat jako nový způsob propagace produktů a služeb, který je založen na schopnosti účinně a interaktivně oslovit cílovou skupinu zákazníků v přesně stanoveném časovém úseku a na předem vybraném místě prostřednictvím atraktivní a dynamické formy komunikace, která zachovává

maximální kvalitu přenášených informací a zároveň minimalizuje časové ztráty a dlouhodobé finanční náklady spojené s jejich změnou či aktualizací.

Z technického hlediska lze Dynamický marketing popsat jako systém vyspělé komunikační sítě, který dokáže prostřednictvím počítače, internetu, mobilní komunikace a přidružených digitálních zobrazovacích zařízení předávat informace a sdělení, dálkově a dle stanoveného časového plánu aktualizovat jejich vysílací schéma na všech uživatelem určených zobrazovacích zařízeních a také aktivně sledovat jejich činnost přes server z jakéhokoli zařízení s internetovým prohlížečem přes internet kdekoliv na světě a v jakoukoli dobu.

Komunikačním výstupním formátem Dynamického marketingu jsou vizuální prezentace, video spoty, reklamní sdělení, informace, digitální TV, živé zprávy pomocí RSS a ostatní multimediální formáty.

Podle zveřejněných výzkumů z roku 2011 společnost Intel predikuje dvouciferný procentuální nárůst zařízení dynamického marketingu. Dále odhaduje počet přehrávačů dynamického marketingu v roce 2015 na 10 miliónů a počet zobrazovacích zařízení využívaných v dynamickém marketingu na 22 miliónů. Podle dalšího výzkumu společnosti Global Industry Analysts se bude globální trh dynamického marketingu v roce 2017 blížit 17 miliardám amerických dolarů [GRANT, MEADOWS, 2012, s. 140]

Navzdory potenciálu a významným nárůstům v počtu instalací, bylo provedeno velice málo empirických výzkumů. Petr Fischer z Ludwig-Maximilians-Universität v Mnichově vypracoval v rámci disertační práce terénní studii u 8 čerpacích stanic, kde studoval vliv dynamického marketingu na prodej různých produktů a služeb v 3 měsíčním cyklu a srovnával výsledky s ekvivalentními měsíci v předešlém roce, ale i s měsíci předcházejícími prováděné studii. Ukázalo se, že dynamický marketing jako efektivní reklamní nástroj má potenciál navýšit, v případě správného používání, prodeje o 10-20% [FISCHER, 2010].

Výhody a potencionální rizika dynamického marketingu

V dnešním multimediálním světě ztrácejí tradiční tištěná média částečně své výhody a účinnost. Nutnost rychlé reakce na požadavky zákazníků, tržní změny a aktivitu konkurence často vede k vyšším nákladům na využití reklamních agentur, na přípravu, výrobu a distribuci tištěných propagačních materiálů. Dynamický marketing tak představuje v současnosti jedno z nejlepších řešení pro firmy, které chtějí pružně reagovat na potřeby zákazníků a aktivně s nimi komunikovat. Mezi hlavní výhody oproti tradičním informačním a reklamním médiím patří rychlost, jednoduchost, variabilita, kreativita a nižší náklady na realizaci a distribuci jednotlivých sdělení.

I přes veliké výhody, které Dynamický marketing nabízí, existuje zde určité riziko, které činí z tohoto komunikačního nástroje potencionálně nebezpečné médium. Tímto rizikem je především bezpečnost.

Vzhledem k tomu, že Dynamický marketing patří mezi média elektronická, musí být zabezpečení na nejvyšší možné úrovni. Získáním přístupových údajů by se mohla stát síť zobrazovacích zařízení nekontrolovatelnou a tím i potencionálně nebezpečnou pro image a dobré jméno jednotlivých společností. Pokud si představíme možnost, že bychom získali práva k síti Dynamického marketingu například mezinárodního obchodního řetězce či k síti

venkovních zobrazovacích zařízení, budeme moci rozhodovat o právě spuštěných prezentacích, měnit obchodní sdělení, ale i dokonce šířit poplašné zprávy.

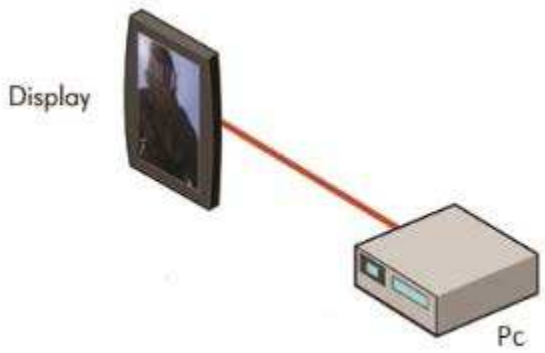
Rozdělení Dynamického marketingu

Dynamický marketing můžeme rozčlenit podle typu umístění a použité technologie k zobrazování obsahu či podle typu technologie využité k samotnému přenosu obsahu. Dynamický marketing avšak primárně rozdělujeme na vnitřní a vnější.

Vnitřní Dynamický marketing využívá v dnešní době většina obchodních center, obchodů, restaurací, nádraží i letišť, neboť jeho vybudování ve vnitřních prostorách je legislativně, technologicky, ale i finančně méně náročné. Hlavní výhoda spočívá v přesném zaměření sdělení cílovému publiku. V případě obchodních prostor cílíme konkrétní sdělení na nakupující, kteří jsou již v obchodě nebo v obchodním centru a jsou ochotni utratit své peníze. Přesně cílenou reklamou tak můžeme oslovit konkrétní cílové publikum s konkrétní nabídkou a to v nejvhodnější okamžik.

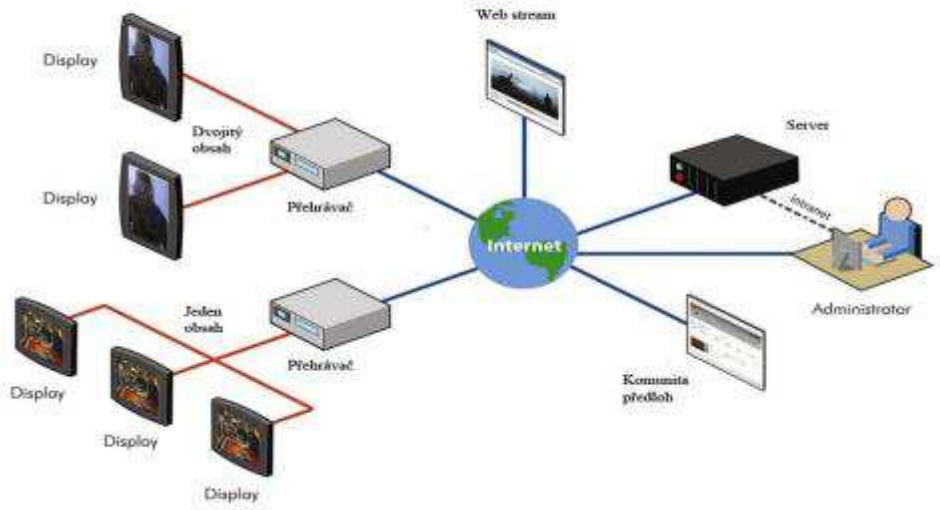
V posledních letech stále více mediálních společností, inzerentů a poskytovatelů obsahu se obrací na vnější velkoplošné digitální zobrazovací zařízení, na venkovní Dynamický marketing. Můžeme je vidět ve formě městských mobiliářů, na straně autobusových zastávek, na zadní části novinových stánků či jako velkoplošných LED zařízení. Jelikož se jedná o venkovní zobrazovací zařízení, je zde potřeba zohlednit několik faktorů. Oproti vnitřnímu prostředí, kde jsou podmínky, mezi něž můžeme zařadit okolní teplotu, osvětlení apod., obecně stabilní, u venkovních zařízení nejsme schopni tyto proměnné ovlivnit. Teploty se v průběhu roku dramaticky mění, musíme počítat s deštěm či sněhem, větrem, vlhkostí vzduchu či všudypřítomným vandalismem. Velikou roli zde hrají i světelné podmínky, které mohou zhoršit viditelnost zobrazovaného obsahu.

Rozlišujeme tři typy Dynamického marketingu podle způsobu přenosu obsahu. Samostatný Dynamický marketing je nejjednodušší formou Dynamického marketingu založeném na propojení jednoho počítače s jedním zobrazovacím zařízením. Počítač není připojen k žádné síti. Obsah zobrazující se na zobrazovacím zařízení je ovládán právě pomocí tohoto jediného počítače. Nový obsah spustíme pomocí USB disku či jiné přenosné paměti. V dnešní době je možné USB disk zapojit přímo do zobrazovacího zařízení a z něj pak přehrávat obsah bez použití počítače.



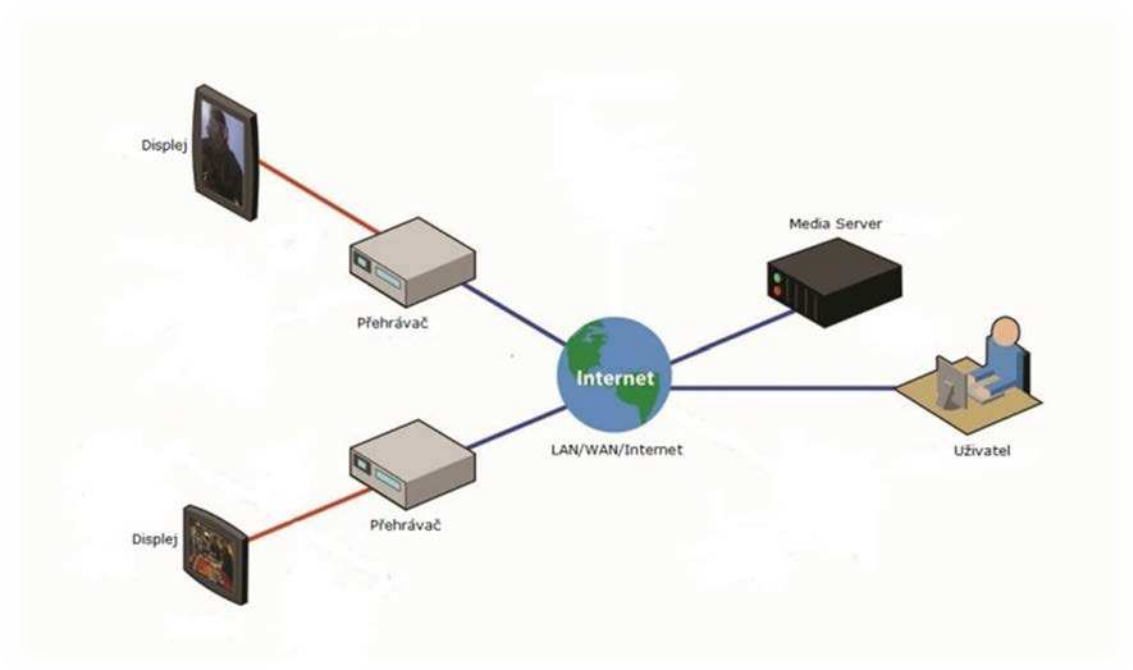
4 Obrázek 4: Samostatný Dynamický marketing

Druhým typem je Webový Dynamický marketing. Zde můžeme obsah, který chceme zobrazovat na zobrazovacím zařízení, řídit pomocí webového prohlížeče přes přímé spojení, které je v síti navázáno s počítačem řídícím přehrávání obsahu či v komplexnějších systémech využít server, který zvládá ovládat až 10 tisíc přehrávačů.



5 Obrázek 5: Webový Dynamický marketing

Třetím druhem je IPTV Dynamický marketing. V tomto druhu Dynamického marketingu je obsah distribuován streamováním médií z média serveru do přehrávačů, které jej distribuují dále do zobrazovacích zařízení. Média server zpracovává veškeré požadavky a řídí samotnou distribuci obsahu. I zde server působí jako klíčový článek systému. Tento přístup je velmi vhodný pro veliké množství zobrazovacích zařízení, které budou zobrazovat limitovaný počet různého požadovaného obsahu.



6 Obrázek 6: IPTV Dynamický marketing

Bezpečnost dynamického marketingu

Bezpečnost Dynamického marketingu musíme rozčlenit do dvou hlavních kategorií: softwarová a fyzická ochrana. Fyzická ochrana je často opomíjena kvůli velikému soustředění se na ostatní prvky bezpečnosti IT systému, jako je ochrana dat před ohrožením různými programy, prolomení hesel či jiných prostředků sloužících k autentizaci.

Různé druhy fyzických útoků a to od jednoduchých, které vyžadují malé znalosti, až po složité útoky, které vyžadují profesionály i značné zdroje, popisuje Steve Weingart. Záměrem je nastínit odpovídající metody ochrany v závislosti na provedeném útoku, složitosti i nákladovosti [WEINGART].

Softwarovou a fyzickou ochranu je také třeba rozdělit podle prvku Dynamického marketingu, na zabezpečení přehrávače a na zabezpečení serveru.

Nejprve si shrneme nejdůležitější body, které musí být dodržovány pro minimalizaci bezpečnostních rizik:

- vyhnout se použití výchozích portů pro běžné protokoly aplikací jako jsou FTP (port 21) nebo web (port 80). Změnit tyto běžné porty na nějaké neobvyklé, například 2122,
- vyhnout se použití běžných hesel jako je „test“ či „jméno“. Je potřeba zvýšit sílu hesla pomocí nejméně 15 znaků s použitím malých a velkých písmen a číslic. Při délce 15 znaků, je entropie přibližně 90 bitů, co je v dnešní době dostatečné. Tato změna znamená podstatné ztížení prolamování hesla hrubou silou. 7 znaků, které se většinou doporučují, s alespoň jedním velikým písmenem a jedním číslem popř. znakem, je entropie pouze 42 bitů. Což při dnešním výpočetním výkonu počítačů trvá rozluštění přibližně 1 hodinu. Při zadání složitějšího a delšího hesla, stoupá pravděpodobnost získání hesla sociálními technikami, neboť lidé budou mít větší tendenci k poznamenání si hesla. Bohužel toto lze velice těžko eliminovat,

- přejmenovat nebo zakázat známé účty. Ve Windows je to účet „Administrator“ a „guest“, v systémech typu Unix „root“,
- povolit nebo nainstalovat firewall. Při konfiguraci povolit pouze ty IP adresy, které musí mít přístup k zařízení. K serveru doporučuji investovat do nákupu firewallu v podobě samostatného hardwaru,
- povolit nebo nainstalovat antivirový software a nezapomenout povolit automatickou aktualizaci,
- stále kontrolovat nejnovější aktualizace softwaru nebo OS a před instalací nezapomenout provádět zálohu,
- pro bezdrátové připojení přehrávačů k síti zakázat bezdrátové SSID (Service Set Identifier) a používat nejnovější šifrovací metody, jako je WPA (Wi-Fi Protected Access),
- nepoužívat při přenášení citlivých dat jako jsou uživatelské jméno a heslo HTTP, ale HTTPS, alespoň se 128 bitovým šifrováním,
- při propojení více přehrávačů používejte síť VPN,
- pokud je využíván přehrávač samostatně bez potřeby připojení k internetu, je potřeba zakázat síťové rozhraní,
- vypnout všechny nástroje pro vzdálenou správu jako jsou Remote Desktop, VNC, PCAnywhere, Telnet nebo SSH, pokud nejsou nezbytně nutné,
- odpojit klávesnici a myš od přehrávače,
- nastavit zámek obrazovky, aby nebylo možno používat přehrávač bez nutnosti zadání hesla.

Důležité je si uvědomit, že bezpečnost musí být řešena při návrhu softwaru i architektury dynamického marketingu, ne dodatečně. Musí se vztahovat na potencionální rizika v kombinaci se správnými bezpečnostními politikami a zahrnovat i bezpečnostní praktiky při skutečném provozu sítě. Důležité bezpečnostní věci, které musí být řešeny v rámci návrhu architektury systému popisuje Michael Willems [WILLEMS, 2008, s.2].

Zabezpečení přehrávače Dynamického marketingu

Zabezpečení přehrávače je většinou řešeno nedostatečně. Společnosti se spoléhají pouze na integrovaný firewall a bezplatný antivirový program. Největší podcenění shledáváme u fyzické bezpečnosti.

Prvním krokem zabezpečení na fyzické úrovni musí být analýza rizik pro daný systém Dynamického marketingu. Je zřejmé, že přehrávač umístěný na odlehlém místě a obsluhující venkovní reklamu bude lákavější cíl než přehrávač umístěný v obchodním centru pod stálým dohledem kamerového systému.

Tento bezpečnostní prvek má funkci zamezit přístupu nepovolaných osob k jednotlivým přehrávačům. Tímto krokem můžeme minimalizovat zcizení majetku, případně poškození hmotného či nehmotného vybavení. Doporučujeme uzavírat přehrávače do uzamykatelných racků, speciálně vytvořených pro konkrétní přehrávač. Pokud se jedná o přehrávače obsluhující venkovní zobrazovací zařízení, doporučujeme instalovat i monitorovací kameru.

U softwarového zabezpečení je nutností přehrávač zabezpečit výkonným firewallem a spolehlivým antivirovým softwarem, pokud chceme minimalizovat riziko ohrožení programem. Do této skupiny můžeme konkrétně zařadit Trojské koně, Logické bomby, Zadní vrátka, Červy, Viry, Bakterie. Obrana proti výše uvedeným metodám spočívá v pravidelné kontrole integrity důležitých souborů, v kontrole přístupových práv, SUID/SGUID souborů či

v nastavení správného vlastnictví důležitých adresářů nebo souborů. Výše uvedené možnosti ohrožení programem platí i pro server. Reálné nebezpečí týkající se bezpečnostních hrozeb serveru je v jiné oblasti.

Zabezpečení serveru

Zabezpečení serveru je v sofistikovanějších systémech Dynamického marketingu klíčovou záležitostí. Server zde obsluhuje přehrávače obsahů a při špatném zabezpečení zde hrozí riziko velkých škod.

Fyzické zabezpečení serveru je hlavní součást bezpečnosti. Řádné fyzické zabezpečení neznamená pouze ochranu dat proti zlodějům či vlastním zaměstnancům, ale hlavně zajištění ochrany před nepředpokládanými událostmi jako je požár a následný zásah hasičského sboru, zemětřesení či poškození elektromagnetického rázu. Pro správné fyzické zabezpečení musí být dodrženy tyto zásady:

- okolo serveru musíme vytvořit bezpečnou oblast vyhrazením například jedné místnosti,
- uložení serveru do racku a následné zamčení,
- při vstupu do místnosti musí každý projít identifikační zónou, jež bude všechny vstupy monitorovat,
- vstup by měli mít povoleni pouze administrátoři či jejich nadřízené osoby.

V dnešní době doporučujeme vzhledem k již relativně nízkým nákladům využít specializovaných firem k uložení serveru či pronájmu serveru dedikovaného. Při dobrém výběru poskytovatele bude náš server fyzicky výborně zabezpečen a navíc budeme moci využít připojení přímo k páteřní síti internetu.

Důležitým aspektem bezpečnosti je šifrování komunikace mezi serverem a přehrávači. Nejrozšířenější metodou systému Dynamického marketingu je šifrování symetrickou šifrou AES (Advanced Encryption Standard) s 256 bitovým klíčem. Při převzetí zprávy přehrávačem je následně za použití kryptografického algoritmu a klíče dešifrována. Musíme si však uvědomit, že šifrováním nemůžeme útočníkovi zabránit v úplném vymazání dat. Dále může útočník změnit šifrovací program tím, že ho modifikuje tak, aby následně používal jiný šifrovací klíč. Musíme vzít v úvahu i možnost luštění. Šifrování musíme tak chápat pouze jako součást bezpečnosti, ale rozhodně ne jako náhradu za ostatní metody používané ke komplexnímu zabezpečení systému.

Všechny systémy Dynamického marketingu využívající server musí řešit bezpečnost serveru webového, přes který řídí své přehrávané obsahy uživatelé. Nejpopulárnější webové servery jsou IIS (Internet Information Services) od společnosti Microsoft a zdrojově otevřený webový server Apache. Mezi bezpečnostní rizika těchto dvou serverů patří zahrnutí spoustu dalších komponent, které některé webové stránky ani nepotřebují a přesto je systémový administrátoři nechávají zapnuté.

Mezi nejznámější patří:

- výpis seznamu adresářů, chybí-li index.html. Tato možnost by měla být zakázána z důvodu usnadnění útočníkovi odhalit nesprávně nakonfigurované soubory nebo adresář, logovací soubory a jiné informace. Musíme si uvědomit, že pokud útočník bude mít možnost správně uhodnout název souboru, bude ho moci také stáhnout,

- nadměrná uživatelská práva. „Svázání naslouchajícího socketu na TCP portu 80 (HTTP) nebo 443 (HTTPS) vyžaduje administrátorskou úroveň práv na většině systémů. Dokud webový server nerestrikuje ty adresáře, které jsou veřejně přístupné, mohou být webovým klientům přístupné také další nezamýšlené adresáře. Z těchto důvodů je po svázání s uvedenými porty většina privilegií webových serverů vypuštěna a snížena na nižší a bezpečnější úroveň“ [ENDORF, SCHULTZ, MELLANDER, 2005, s.105],
- symbolické linky. Útočník může získat přístup k citlivé části souborového systému pomocí prohledávání symbolických linků. Tato vlastnost by proto měla být vypnuta.

Útok na dostupnost služeb považujeme za největší hrozbu Dynamického marketingu. Vzhledem k jeho centralizaci do jednoho místa, čili serveru, který obsluhuje všechny přehrávače, se stává lehce zranitelný útokem známým jako Denial of Service, ve zkratce útok DoS.

Způsob útoku formou DDoS se v poslední době stává velikou bezpečnostní hrozbou nejenom elektronického obchodu. Distribuovaných útoků (Distributed Denial of Service, DDoS) se účastní veliké množství počítačů, tzv. zombie sítě (Botnet), které jsou většinou využívány bez vědomí majitele, k zahlcení kapacity i nejmodernějších linek. V dnešní době je obrana proti tomuto druhu útoků velmi obtížná nejenom z vyplývajícího faktu, že napadnuté servery s tímto útokem v danou chvíli nepočítají, ale i vzhledem k objemu dat, se kterými pracují.

V dnešní době mezi moderní útoky se řadí přímá cesta vyčerpání veškeré kapacity oběti, tudíž jakýkoli požadavek legitimního uživatele nebude vyslyšen. Do této skupiny můžeme zařadit:

- zaplavování SYN pakety,
- zaplavování UDP pakety,
- zesilovače. Do této skupiny řadíme Smurf a Fraggle.

Proti těmto útokům se brání zakázáním všesměrového vysílání.

Nejdříve byly velice populární DoS útoky, které vyčerpaly veškerou kapacitu oběti. Nyní se stává velice moderním útoky na aplikační vrstvu, kde útočník nemusí mít k dispozici velkou kapacitu linky. „Základní scénář útoku na aplikační vrstvě je jednoduchý. Nejprve musí útočník najít nějakou veřejně přístupnou síťovou službu oběti s výrazným nepoměrem mezi náročností dotazů a náročností odpovědí. Pak stačí posílat každou vteřinu několik dotazů a výpočetní složitost služby oběť spolehlivě složí. Nejhorší z našeho pohledu je, že se útok vyhne většině opatření proti DoS útokům, takže nalezení příčiny zátěže a zdroje útoku vyžaduje drahou a pomalou ruční práci“ [MCCLURE, SCAMBRAY, KURTZ, 2007, s. 394].

Můžeme využít technologie pro obranu proti DoS útokům například Cisco Guard či Top Layer. Mezi směrovače s dobrou pověstí řadíme směrovač Juniper, který zvládá i filtrování rychlosti linky. Tyto produkty umí výrazně omezit běžné DoS techniky typu SYN paketů nebo zaplavování požadavky na HTTP spojení.

Přes veškeré výše uvedené kroky nebudeme schopni zcela zamezit těmto typům útoků, proto by celý systém měl být navržen takovým způsobem, aby se účinky útoku typu DoS co nejvíce eliminovaly. Proto při vývoji či koupi systému musíme brát zřetel na systémové rozvržení prvků Dynamického marketingu. Zde doporučuji při rozsáhlejších projektech

využívat takové systémy, které si přehrávaný obsah ze serveru pravidelně aktualizují na přehrávače.

7 Celá problematika zabezpečení IS organizace je velice široká. Všechny bezpečnostní hrozby, kterým čelíme každý den, samozřejmě hrozí všem prvkům Dynamického marketingu. Je alibistické si říci, že pokud se staly terčem úspěšných pokusů o napadení servery státních, vojenských či jiných institucí, máme mizivou naději těmto útokům čelit. Musíme si ale uvědomit, že za každým napadením stojí lidská chyba. Ať v nedostatečné obezřetnosti, ve špatném nastavení systémů, nedostatečné aktualizaci tak i v nedostatečné kvalifikaci.

Potencionální škody v Dynamickém marketingu

Michael Callahan, víceprezident marketingových řešení společnosti HP řekl: „ Organizace vydávají stále větší množství času, peněz a energie v reakci na zvyšující se úroveň kybernetických útoků, jež se brzy stane neudržitelná. Existují jasné důkazy, že nasazení pokročilých inteligentních řešení pomáhá výrazně snížit nejenom náklady, ale i četnost a dopad těchto útoků“ [HP, 2012, s.1]. Při prolomení bezpečnosti aplikace Dynamického marketingu je třeba možné škody z technického hlediska rozdělit do dvou částí, a to na škody způsobené prolomením bezpečnosti na serveru a na škody způsobené prolomením bezpečnosti na přehrávačích.

Prolomení bezpečnosti na serveru může proběhnout dvěma způsoby, a to vyřazením serveru z provozu, čehož lze docílit útoky typu DoS, které jsme si popsali výše, nebo převzetím kontroly nad serverem.

Škoda způsobená vyřazením serveru z provozu**.** Server obsluhuje konkrétní počet přehrávačů, kterým rozesílá obsah, který přesně určené přehrávače Dynamického marketingu zobrazují. Tento obsah si přehrávač stáhne pomocí FTP k sobě na pevný disk a dále ho zobrazuje podle typu naplánování. Po určeném čase se přehrávač zeptá serveru, zda je zobrazovaný obsah změněn. Pokud dostane kladnou odpověď, stáhne si přehrávač aktualizovaný obsah. V případě vyřazení serveru, by veškeré přehrávače pokračovali v zobrazování stávajícího obsahu. Pro minimalizaci škod doporučujeme mít server pod stálou kontrolou, aby potencionální obnovení činnosti serveru proběhlo v co nejkratším čase. Při větším problému by měl být k dispozici server záložní, který jakoukoli změnu v datové oblasti způsobenou změnou předloh od uživatelů provádí synchronizací této části dat. Velké škody nastávají v IPTV Dynamickém marketingu, který veškerý zobrazovaný obsah streamuje ze serveru. Po vyřazení serveru z provozu jsou vyřazeny i zobrazovací zařízení a nastává zde celkový výpadek sítě IPTV Dynamického marketingu.

Škoda způsobená převzetím kontroly nad serverem. Způsobená škoda se odvíjí od doby převzetí kontroly útočníkem do doby odstavení serveru a spuštění serveru záložního. Každá společnost by měla mít vypracované schéma Bezpečnosti řízení, kde by se měla pohybovat doba od převzetí k opětovnému spuštění maximálně mezi 10-15 minutami. V tomto časovém horizontu by útočník byl schopen spustit vlastní obsah do sítě přehrávačů pod jednotlivými uživateli. Zde je potřeba zmínit, že bezpečností pravidla v systému by měla být nastavena tak, aby nebylo možné spustit na všechny přehrávače ovládané serverem stejný obsah najednou, ale i v případě administrátora pouze pod účtem uživatele. Velikost škody by zde závisela na počtu přehrávačů pod jednotlivými uživateli. Pokud například budeme uvažovat 200 zobrazovacích zařízení pod kontrolou útočníka po dobu 10 minut, tak se výše škody

z hlediska nákladů na pronajatý inzertní prostor odvíjí od frekvence a počtu jednotlivých reklamních sdělení. Jestli budeme uvažovat například spot o délce 30 sekund, 12 inzerentů, cenu za 30 sekund reklamního času cca 5 Kč za jednu obrazovku, pak škoda představuje pro pronajímatele reklamního prostoru ztrátu příjmu ve výši 20 000 Kč. Pro inzerenty však může být výše škody o hodně vyšší, protože během 10-ti minut může dojít k poškození image značky inzerenta v případě vysílání nežádoucích reklamních sdělení. Škoda závisí na počtu osob „přijímajících" v daný okamžik obchodní sdělení. V případě prolomení bezpečnosti serveru a vysílání nežádoucích sdělení je potřeba brát v úvahu také riziko vzniku možné paniky ze strany „příjemců" poplašných sdělení, jejichž důsledkem může vzniknout vysoká škoda v podobě ušlého zisku, ale především z hlediska ochrany obyvatel. Zde můžeme zahrnout zavření obchodního centra v důsledku poplašné zprávy, zdravotní následky při následném chaosu, újmy na majetku apod. (podle § 357 trestního zákoníku č. 40/2009 sb., je šíření poplašné zprávy trestním činem).

Při převzetí kontroly nad přehrávačem Dynamického marketingu se škoda znovu pohybuje podle typu umístění a počtu zobrazovacích zařízení připojených k přehrávači. Zde se doba k opětovnému převzetí kontroly nad přehrávačem odvíjí podle způsobu převzetí útočníkem. Při stálém připojení k internetu lze přehrávače ovládat pomocí serveru a napadnutý přehrávač tak vypnout. Při odpojení internetu útočníkem existuje pouze možnost osobního vypnutí. V tomto případě se doba opětovné kontroly nad přehrávačem pohybuje v časovém horizontu potřebnému pro dojezd na místo uložení přehrávače. Toto se týká pouze přehrávačů umístěných na velkoplošných zobrazovacích zařízeních mimo obchodní centra. V Praze se konkrétně jedná o zobrazovací zařízení umístěná solitérně okolo frekventovaných silnic. Škoda zde způsobená se opět odvíjí od obsahu, který útočník na zobrazovací zařízení umístí. Zde platí stejné možnosti jako v případě převzetí serveru. Liší se ale počtem zobrazovacích zařízení.

Na závěr bychom chtěli připomenout, že mimo škodu způsobenou přehrávaným obsahem je vždy třeba brát v úvahu ztrátu image společnosti a tudíž i možnost jejího zániku. Konkrétní finanční škoda tedy není přesně vyčíslitelná, neboť vždy záleží na dané situaci, velikosti firmy a její známosti.

Literatúra a zdroje

GRANT, August, MEADOWS, Jennifer: Communication Technology Update and Fundamentals. 1.vyd. Waltham: Focal Press, 2012, s.140. ISBN 978-0-240-82456-7.

ENDORF, Carl, Eugene SCHLUTZ a Jim MELLANDER. *Detekce a prevence počítačového útoku*. 1. vyd. Praha: Grada, 2005, s. 102, s. 105. ISBN 80-247-1035-8.

HP: *HP Research: Cybercrime Costs Rise Nearly 40 Percent, Attack Frequency Doubles*.[online]. Pablo Alto: HP, 2012. Dostupné na: http://www.hp.com

WILLEMS, Michael: *Security in Digital Signage Technology*. [online]. Toronto: Enqii, 2008.

Dostupné na:
http://www. dailydooh.com/wp-content/uploads/2008/03/security_white_paper.pdf

FISCHER, Peter: *Digital Signage – Werbliche Kommunikation am Point of Sale auf Flachbildschirmen. Theoretische Hintergründe, Aufgaben und Wirkungsmessungen.* [online] München: Ludwig-Maximilians-Universität, 2010.
Dostupné na http://edoc.ub.uni-muenchen.de/12844/1/Fischer_Karl_Peter.pdf

WEINGART, Steve*: Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses*. [online]. Hawthorne: IBM. Dostupné na http://link.springer.com/content/pdf /10.1007%2F3-540-44499-8_24.pdf

MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking bez záhad*. 1. vyd. Praha: Grada, 2007, s. 394. ISBN 978-80-247-1502-5.

Bc. Zdeněk Freund
RNDr. Jan Lánský, PhD.
Vysoká škola finanční a správní
Fakulta ekonomických studií
Estonská 500
101 00 Praha 10
21169@vsfs.cz

Tento výzkum byl podporován Specifickým vysokoškolským výzkumem Vysoké školy finanční a správní, 2013.