

SecureMail iStor

Kako radi?

SecureMail upravljani servis tipično će blokirati 99% - 99,5% spam poruka, uz malu vjerojatnost da će blokirati legitimne e-mail poruke. Osim očitih prednosti poput uštede vremena, servis ima i dodatne prednosti:

- smanjuje potrošenu propusnost Internet veze do Vašeg internog e-mail servera. Uštede po ovom pitanju često su veće od cijene ovog servisa!
- Smanjuje mogućnost krađe identiteta i brojeva kreditnih kartica
- Antivirus smanjuje mogućnost virusne infekcije, što bi tvrtku značajno koštalo
- Smanjuje broj izgubljenih e-mail poruka putem prikupljanja i centraliziranog slanja (spooling) poruka u slučaju da je mail server nedostupan.
- Omogućuje korištenje osobne 'crne liste' kako bi se blokirale neželjene poruke.
- Gotovo u potpunosti eliminira pornografiju i ostale vulgarne e-mail poruke koje su uvredljive za većinu ljudi

Mehanizmi koje SecureMail koristi za blokiranje Spam-a

Tehnologija prepoznavanja obrazaca koji se ponavljaju (Recurrent Pattern Detection Technology - RPD)

Umjesto da procjenjuje svaku pojedinačnu poruku, RPD tehnologija analizira velike količine Internet prometa u realnom vremenu. Pojava novih vrsta spam-a i zlonamjernih softvera prepoznaju se čim se pojave te se informacije o njima spremaju u repozitorij opisa (Signatures Repository). RPD tehnologija efikasna je za sve jezike i formate. Ona pruža zaštitu u realnom vremenu od samog pojavljivanja nove prijetnje, što osigurava trenutnu zaštitu od pojavljivanja novih prijetnji – prije dohvaćanja novih opisa ili softverskih nadogradnji. (RPD je dostupan samo na razini servisa.)

Mehanizam bodovanja (heuristika i bayesian)

Posjedujemo preko 3000 skupova pravila koji se neprestano nadopunjavaju u svrhu otkrivanja pojave novih vrsta spam-a. Ovo je omogućeno butem bayesiane tehnologije koja koristi umjetnu inteligenciju za svrstavanje e-mail poruka u spam. Ova tehnika dodjeljuje određen broj bodova poruci na temelju heurističke analize te svrstava poruku kao spam ovisno o ukupnom broju bodova.

Filtriranje pomoću 'crne liste' , u stvarnom vremenu

Nekoliko organizacija i tvrtki neprestano prepoznaju e-mail poslužitelje koji aktivno šalju spam poruke. One kreiraju 'crne liste u stvarnom vremenu' (real-time blacklists – RBL) uz pomoć IP adresa tih poslužitelja koje se ažuriraju dnevno, pa čak i unutar nekoliko sati. Odabrali smo pet poznatijih RBL-ova koje koristimo za SecureMail servis (po nazivnim postavkama, odabrano je svih pet listi). Glavni kriterij za odabir su liste za koje je najmanje vjerovatno da će blokirati legitimne e-mail poruke.

Provjere otisaka (prepoznavanje obrazaca koji se ponavljaju, DCC)

Ova tehnika koristi se za klasificiranje skupova poruka. Temelji se na konceptu prema kojem je mogućnost da se radi o spamu veća što više jednakih poruka kruži Internetom.

URL provjere

Ovaj sustav analizira url-ove koji se nalaze unutar poruka i uspoređuje ih s bazom podataka o poznatim domenama koje šalju neželjene poruke. Ova tehnika prepoznaje kako spam tako i tzv. 'phising' prijevare.

DNA provjere (Razor)

Pošiljatelji spam poruka obično modificiraju spam sadržaj kako bi izbjegli otkrivanje. Tehnika DNA provjere prepoznaje promjene i povezuje varijacije u bazi podataka poznatih spam poruka.

Filtriranje sadržaja

- Dopusća ili uskraćuje pristup privicima e-mail poruka ovisno o nazivu datoteke, uz upotrebu bilo koje politike e-mail sigurnosti. Služi za jednostavno blokiranje privitaka koji su često zapravo zamaskirani virusi, npr. ReadMe.doc.exe. Liste ovakvih privitaka mogu se modificirati prema potrebama pojedinačnih korisnika.

- Filtriranje napada temeljenih na HTML-u

- Pronalaženje čestih znakova napada poput <iframe> i <Object Codebase=...> HTML oznaka. Obje ove oznake mnogo puta su bile primjenjivane za iskorištavanje sigurnosnih propusta u Outlook-u i Internet Explorer-u.

- Potencijalno opasan HTML sadržaj može se ukloniti. Provjere i 'zamke' dodane su za sve poznate sigurnosne propuste za Outlook, Outlook Express, Internet Explorer i Eudora-u.

'Bijele' i 'crne' liste

Iako naši servisi ne zahtijevaju 'fino podešavanje' ili 'učenje', te je mala vjerojatnost da će blokirati legitimne e-mail poruke, moguće je osigurati da važni klijenti i kontakti nikada ne budu blokirani, na način da ih se doda u 'bijelu listu' specifičnu za zadanu domenu. Ovo je posebno korisno ako postoji malen broj klijenata u državama iz kojih je uglavnom poželjno blokirati poruke.

Naprimjer, neki od naših klijenata imaju mnogo kontakata u Kini. Odabrali su dodati te kontakte u svoju 'bijelu listu', a sve ostale poruke iz Kine odlučili su blokirati.

Kontakte se na 'bijelu listu' može dodati prema kriteriju e-mail adrese, nazivu domene, IP adrese ili sadržaja. Kako bi se dodatno smanjila mogućnost da e-mail poruke iz legitimnih izvora budu blokirane, mi održavamo globalnu 'bijelu listu' za sve naše klijente. Tvrtke s velikim mailing listama klijenata ponekad budu stavljene na 'crnu listu' samo zbog velike količine e-mail poruka koje šalju. Mi dodajemo te i druge provjerene tvrtke na globalnu 'bijelu listu'. Rado ćemo u obzir uzeti prijedloge naših klijenata, koji se mogu poslati putem upravljačke ploče.

Također se može koristiti i prilagođena 'crna lista' kako bi se spriječilo nekoga da maltretira Vaše zaposlenike. Također možete blokirati 'kradljivce kadrova', mailing liste ili bilo koga drugoga za koga ne želite da kontaktira Vaše zaposlenike. Zapisi u 'crnu listu' mogu se vršiti prema e-mail adresi ili IP adresi.

Ne preporučamo da klijenti sami pokušavaju blokirati preostale (nefiltrirane) spam poruke (za razliku od drugih anti-spam sustava). Umjesto toga, nefiltrirane poruke bi trebalo poslijediti nama i naše osoblje će odmah kreirati najprikladniji filter za njih.

Riječničke provjere

Riječničke provjere mogu zadovoljiti sve posebne potrebe. Naprimjer, ako Vaša kompanija stvori proizvod pod nazivom „MasterWidget“ možete dodati filter u 'bijelu listu' koji će omogućiti prihvaćanje svake e-mail poruke koja sadrži taj pojam.

Također možete kreirati filter koji će odbaciti svaku e-mail poruku koja sadrži pojam „Viagra“.

Mehanizmi koje iStor SecureMail koristi u blokiranju virusa

Traženje virusa trostruke razine

Ovaj mehanizam pregledava sve e-mail poruke za viruse pomoću tri različita antivirusna softvera kako bi osigurao najveću zaštitu.

Trenutna virusna zaštita

Proaktivnim pretraživanjem Interneta i prepoznavanjem višestrukih pojavljivanja virusa čim se dogode, trenutna zaštita omogućuje proaktivno blokiranje virusa koje je efikasno i neovisno o opisima virusa. Ovo rješenje efikasno rješava ranjivosti odmah nakon pojave novih virusa, kada se zaraze milijuni korisnika. Proaktivno prepoznavanje virusa osigurava zaštitu korisnika, satima prije nego se objave opisi novih virusa.

- Privici koji sadrže viruse i ostale sigurnosne rizike uklanjaju se.
- Svi sigurni sadržaji isporučuju se nepromijenjeni

Iako će ovaj servis ukloniti veliku većinu poznatih e-mail virusa, virusi također mogu inficirati računala drugim načinima. Za najveću zaštitu preporučujemo korištenje antivirusnog softvera na svakom računalu. Iako nijedna usluga ili softver ne može jamčiti zaštitu od svih virusa, SecureMail nudi dodatnu razinu zaštitu od virusa.