

Användningen av Sender Policy Framework bland svenska börsbolag

April 2009

Exekutiv sammanfattning

När man skickar e-post gör standardprotokollet SMTP ingen kontroll av avsändaradressen och dess giltighet. Detta innebär att vem som helst kan skicka ett e-post som ser ut att komma från exempelvis `fornamn.efternamn@foretag.se`, trots att personen inte har någon som helst koppling till `foretag.se`. Detta kan utnyttjas av spammare och bedragare, och har utnyttjats vid angrepp mot svenska toppchefer på börsnoterade bolag. Redan för sex år sedan (2003-2004) formulerades en standard för att bemöta problemet. Så småningom fick standarden namnet Sender Policy Framework (SPF).

Vi har undersökt hur bred användning SPF har fått i Sverige. Undersökningen har gjorts dels i bredd på cirka 12 000 domäner, dels på alla registrerade bolag på Stockholmsbörsen OMX. Våra resultat visar att SPF fortfarande inte används i någon större utsträckning. Endast 3 av 10 bolag på Large Cap-listan använder SPF. Användningen är sedan fallande med cirka 2 av 10 för Mid Cap och Small Cap samt 1 av 10 för vårt stora urval av domäner.

Vår spekulation kring att stora bolag i större utsträckning använder SPF är att de har en större genomströmning av extern kompetens i kombination med en större tillgång på intern kompetens specialiserad för både e-post och säkerhet.

Vi ser det som särskilt bekymrande att SPF inte har fått en bredare användning eftersom det idag förekommer attacker som utnyttjar bristen. Våra resultat visar således inte bara att en stor andel av börsbolagen misslyckas med att leva upp till best practice, man missar också att använda enkla medel för att svara på verkliga angrepp.

Innehåll

Exekutiv sammanfattning.....	2
Inledning.....	4
Hur SPF fungerar	4
Vad SPF skyddar mot.....	5
Skydd mot spam	6
Skydd mot bedrägerier.....	6
Vad SPF inte skyddar mot.....	7
Tidigare undersökningar.....	7
Metod.....	7
Börsbolag från OMX	8
Generellt svenskt urval.....	8
Filtrering	8
Resultat.....	9
Analys	9
Svagheter med metoden.....	9
Förfalskad e-post.....	10
Korrelation mellan bolagets storlek och SPF.....	11
Användningen av SPF	11
Man måste vara två.....	11
Stora miljöer	11
E-post är det viktigaste vi har.....	12
Skyddar mot attacker som är förhållandevis okända.....	12
Slutsats	12
High Performance Systems	12

Inledning

Sender Policy Framework förkortas SPF och definierades formellt för första gången i RFC (Request For Comments) 4408 som publicerades i april 2006. Det har dock använts i praktiken ända sedan början av 2004. Tidigare undersökningar har visat att det även togs till praktisk användning under 2004, då en majoritet av Fortune 1000-företagen implementerade SPF. Mer om detta återfinns i under rubriken *Tidigare undersökningar* på sidan 7.

Hur SPF fungerar

För att förstå hur SPF fungerar krävs en grundläggande förståelse för hur e-post skickas över Internet. I stort sett all e-post på Internet skickas med hjälp av Simple Mail Transfer Protocol (SMTP). Lyckligtvis så är det traditionella postsystemet i vår fysiska värld en bra analogi till hur SMTP fungerar. Avsändaren skriver ett brev, lägger det i ett kuvert och skriver mottagaradress samt avsändaradress på kuvertet. Avsändaren lägger sedan kuvertet i en postlåda (avsändarens e-postserver), därefter tar Posten över och ser till att det hamnar i mottagarens brevlåda (mottagarens e-postserver) varifrån mottagaren kan hämta, öppna och läsa brevet. Notera att det är fritt fram för avsändaren att skriva vilken avsändaradress som helst (eller ingen alls) på kuvertet. Precis samma sak gäller för e-post på Internet. SPF syftar till att hindra förfalskningar av avsändaradresser på kuvert genom att en organisation kan reglera vilka som får utge sig för att skicka från den.

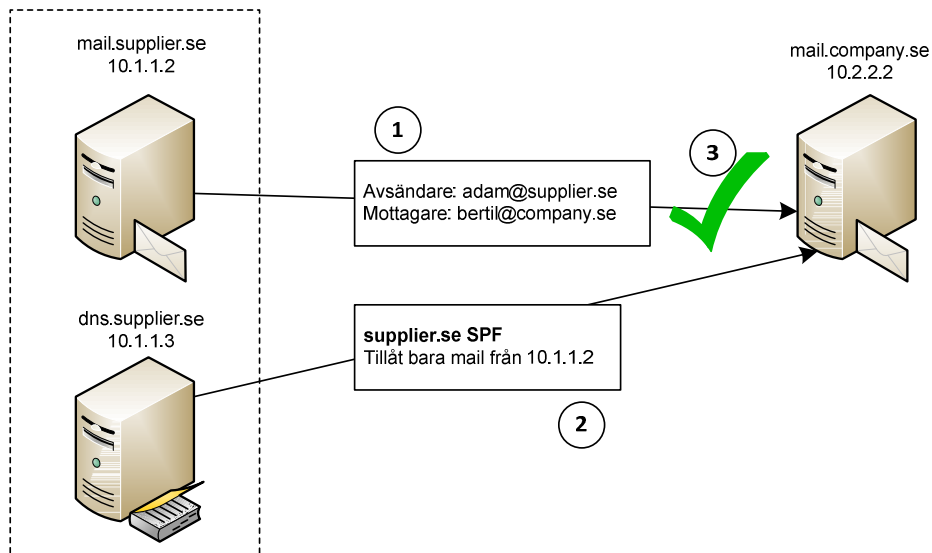
Den grundläggande idén med SPF är att ägaren av en domän ska kunna begränsa vilka som får skicka e-post från den domänen. Ägaren av example.com gör detta genom att publicera en lista på vilka Internetadresser avsändare på example.com använder. Mottagaren av ett e-postmeddelande som verkar komma från example.com kan då kontrollera dess lista och om ursprunget inte stämmer med vad listan säger ignoreras meddelandet. Ägaren av foretag.se kan alltså hindra utomstående från att använda till exempel vadsomhelst@foretag.se som avsändaradress.

För att SPF ska användas mellan två parter måste båda vara engagerade i protokollet. Två aktiviteter krävs; (1) avsändaren måste ha SPF-regler publicerade för sin domän i förväg och (2) mottagaren måste kontrollera dessa regler när e-post tas emot. Avsändare och mottagare åtnjuter sedan olika sorters skydd av SPF:

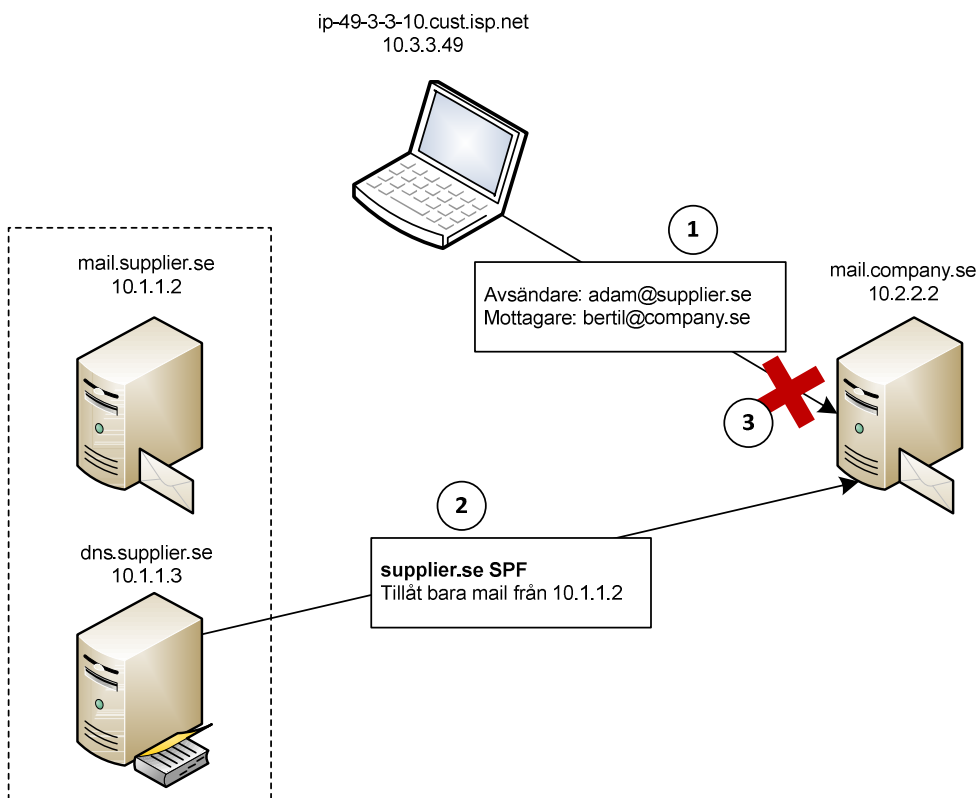
- Avsändare kan hindra obehöriga från att utge sig att vara dem.
- Mottagare kan undvika att bli lurade av förfalskade avsändare.

Det är viktigt att påpeka att både avsändare och mottagare måste vara delaktiga i en transaktion annars har ingen av dem nytta av SPF. Två exempel; (1) Företag A har SPF-regler publicerade, om mottagaren inte kontrollerar dessa när e-post tas emot från foretaga.se så har de ingen effekt. (2) Företag B har däremot inga SPF-regler publicerade så mottagare av e-post från foretagb.se kan inte kontrollera dem.

Nedan visas två illustrerade fall (Figur 1 och Figur 2) där (1) e-post tas emot, (2) SPF-regler kontrolleras och e-post (3) accepteras respektive nekas.



Figur 1: E-post tas emot efter kontroll av SPF-regler.



Figur 2: E-post nekas efter kontroll av SPF-regler.

Vad SPF skyddar mot

SPF erbjuder en möjlighet att skydda mot spam och bedrägerier där avsändaradressen är förfalskad.

Skydd mot spam

SPF är inte i första hand ämnat för att minska spam men erbjuder implicit ett visst skydd i samband med att avsändaradressen förfalskas. En undersökning¹ från 2004 visade att endast 3 % av all spam som skickades kunde stoppas med hjälp av SPF.

Spam med förfalskad avsändaradress

Spam skickas sällan eller aldrig med den egna avsändaradressen utan i regel används en förfalskad adress. Om ägaren av den domän där den förfalskade adressen ligger använder sig av SPF har mottagaren möjlighet att filtrera bort den oönskade e-posten.

Notera dock att SPF i första hand inte är ett verktyg för att minska spam. Spammare kan enkelt gå runt skyddet genom att använda en avsändardomän som inte använder SPF eller helt enkelt registrera en ny domän med tillåtande SPF-regler. Den stora fördelen med SPF i samband med spam är istället möjligheten att minska "backscatter".

Minskning av backscatter

Ibland skickas svar på e-post automatiskt tillbaka till avsändaren. Detta kan bero på e-postadresser som inte existerar vilket leder till att den mottagande e-postservern skickar tillbaka ett felmeddelande. Det kan också bero på så kallade "out-of-office replies" där mottagarens e-postprogram automatiskt skickar ett svar och förklarar att denne inte kan besvara meddelandet just nu.

När en spammare har förfalskat en avsändaradress, skickar 100 000 e-postmeddelanden och en procent av dessa resulterar i ett felmeddelande eller ett out-of-office reply innebär det att 1 000 svar kommer att hamna i den förfalskade avsändarens brevlåda. Detta fenomen kallas *backscatter*.

Om ägaren av den domän som har använts som förfalskad avsändaradress har implementerat SPF kommer de mottagande e-postserverna kunna kasta meddelandet på en gång och därmed genereras inget backscatter.

Skydd mot bedrägerier

Med bedrägerier avses här sådana som baseras på kommunikation där avsändaren utger sig för att vara någon annan. Med SPF går det att skydda sig mot att ta emot e-post med förfalskad avsändare och att någon annan skulle utge sig för att skicka e-post som kommer från ens egen domän.

Förfalskning av andra domäner – inkommande e-post

Genom att kontrollera inkommande e-post och matcha vem som skickar mot avsändardomänens SPF-regler kan e-postbedrägerier med förfalskad avsändaradress stoppas. Detta kräver att avsändardomänen har SPF-regler definierade, vilket man alltså kontrollerar för att man själv inte ska ta emot e-post med falsk avsändare.

¹ http://www.ciphertrust.com/resources/statistics/spf_stats.php

Förfalskning av den egna domänen – utgående e-post

Om mottagaren av e-post kontrollerar SPF-regler enligt ovan kan man skydda sig mot bedrägerier där den egna domän används som avsändare genom att publicera lämpliga SPF-regler. Detta gör man då för att andra inte ska kunna skicka e-post där man själv står som (förfalskad) avsändare.

Vad SPF inte skyddar mot

Det är viktigt att poängtera att SPF endast auktoriserar avsändardomänen som anges på e-postmeddelandets kuvert² och inte de i brevhuvudet som till slut hamnar hos klienten. Användande av SPF gör alltså inte att man kan lita på avsändaradressen i brevhuvudet, endast på kuvertets adress.

Samtidigt som SPF skyddar mot exakta förfalskningar skyddar det inte mot att en avsändare med liknande adress används. Istället för att sända från foretag.se kan kanske e-post skickas från foretag.com eller foretag.se. Dessa domäner behöver inte ens existera för att kunna användas som avsändaradress. Finns inte domänen så finns förstås inte heller några regler för SPF publicerade. Å andra sidan finns där den uppenbara kontrollen att ställa frågan om det finns en e-postserver (MX-record) som kan ta emot återvändande e-post, vilket det naturligtvis inte finns i det läget.

Ytterligare en attack som SPF inte kan (eller är designad för att) skydda mot är förfalskning av användarnamnet i e-postadressen. Det är till exempel fullt möjligt för användaren adam på foretag.se där det finns SPF-regler att skicka e-post som ser ut att komma från bertil@foretag.se.

Tidigare undersökningar

En undersökning³ gjord av CipherTrust visade att i oktober 2004 använde 54 % av Fortune 1000-företagen SPF. Samma undersökning konstaterade att SPF inte var ett effektivt sätt att stoppa spam, även om en liten del stoppades. Dess bästa användningsområde var att förhindra ”spoofing och phishingangrepp”. Infoblox gjorde en undersökning⁴ 2006 där man undersökte cirka två miljoner .com- och .net-domäner. Man kom fram till att endast 5 % av dessa hade SPF-regler publicerade. oktober 2007 publicerade⁵ Infoblox att 12,6 % av omkring två miljoner testade domäner hade SPF-records. Ytterligare en studie⁶ från Infoblox i november 2008 säger att det föregående årets användning hade ökat från 12,6 % till 16,7 %.

Metod

Undersökningen riktar in sig på bolag som är registrerade på svenska OMX börsen, dessa jämförs sedan mot ett generellt urval.

² De domäner som anges i HELO och MAIL FROM och alltså inte t ex From i brevhuvudet.

³ http://www.ciphertrust.com/resources/statistics/spf_stats.php

⁴ http://www.infoblox.com/library/pdf/dns_report_card.pdf

⁵ <http://dns.measurement-factory.com/surveys/200710.html>

⁶ <http://www.infoblox.com/news/release.cfm?ID=132>

Börsbolag från OMX

Hemsidor för samtliga bolag på OMX listor Large Cap, Mid Cap och Small Cap söktes upp manuellt med hjälp av sökmotorer. Från hemsidan identifierades sedan vilken domän som användes för att skicka e-post. I fallet då fler domäner användes valdes den som verkade ha flest kontakter knutna till sig. De domäner som identifierades sparades i separata filer för Large, Mid respektive Small.

Generellt svenskt urval

För att kunna jämföra resultatet från börsnoterade bolag behövs ett urval av domäner som används av generella, svenska användare. Detta kräver andra källdata som sammanställdes från ett par av de användardatabaser som har läckt ut efter intrång i svenska community-sidor under 2008 och 2009. De användardatabaser som fick utgöra källdata är:

- Bilddagboken
- Dataföreningen
- Efterfesten
- Anstalten.nu
- Travpunkten.com
- DIF Hockey

Samtliga fält för e-postadresser som matchade följande reguljära uttryck plockades ut från de råa databasdumparna:

```
^[0-9a-zA-Z]([-.\w]*[0-9a-zA-Z_+])*@[0-9a-zA-Z]([-.\w]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,9}$
```

Uttrycket är hämtat från *Regular Expression Pocket Reference* från O'Reilly och matchar korrekta e-postadresser. Från dessa adresser klipptes sedan domännamnet av och sparades i en separat fil.

Filtrering

För samtliga domäner hämtades dess respektive TXT-record och sparades i en lista. Domäner som inte existerade (svarade med `NXDOMAIN`) raderades från listan. Från de återstående noterades antalet domäner som returnerade ett TXT-record som innehöll strängen `"v=spf1"`. De domäner som noteras anses ha publicerat regler som kan kontrolleras av utomstående enligt SPF. Se Figur 3 nedan där `nslookup` används för att visa SPF-regler offentligtgjorda av HPS för `hps.se`.



```
cmd - nslookup - 208.67.222.222
C:\>nslookup - 208.67.222.222
Default Server: resolver1.opendns.com
Address: 208.67.222.222

> set type=txt
> hps.se
Server: resolver1.opendns.com
Address: 208.67.222.222

Non-authoritative answer:
hps.se text =
        "v=spf1 ip4:217.118.223.0/26 ip4:10.172.100.0/24 -all"
>
```

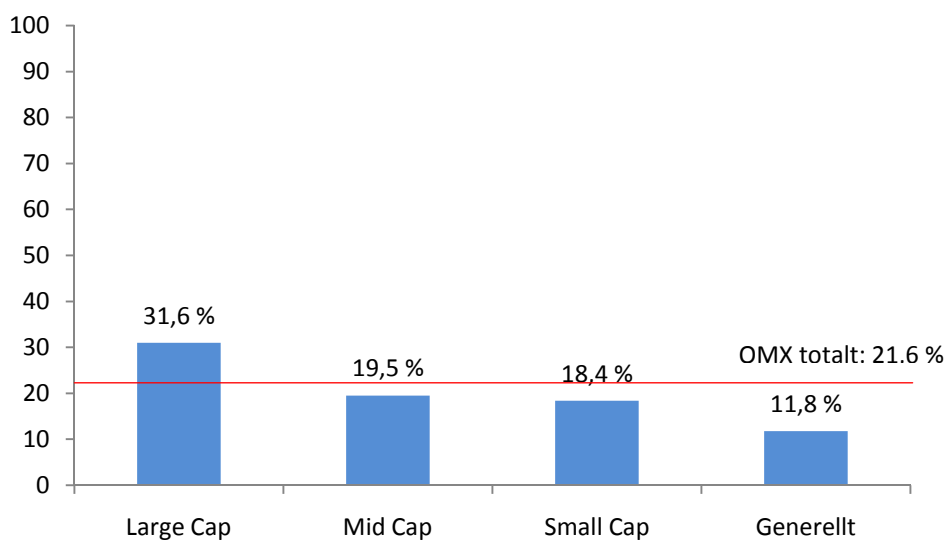
Figur 3: TXT kontrolleras för `hps.se` via DNS.

Resultat

Nedan presenteras resultatet från undersökningen i tabellformat och som stapeldiagram i Figur 4 respektive Figur 5.

	Antal med SPF	Antal totalt	Andel SPF
Large Cap	18	57	31,6 %
Mid Cap	15	77	19,5 %
Small Cap	23	125	18,4 %
Totalt OMX	56	259	21,6 %
Generella domäner	1419	11996	11,8 %

Figur 4: Resultat från undersökningen fördelat på urval.



Figur 5: Andel av börsbolag som har publicerat SPF-regler.

Analys

Svagheter med metoden

Databasdumparna som har använts för att representera ett generellt urval av domäner som nyttjas av svenskar innehåller en okänd mängd påhittade adresser. Till exempel kan det komma av användare som provar att registrera ett konto med en fiktiv adress. Antingen är denna adress helt

ogiltig eftersom dess domän inte existerar eller så sammanfaller det med en domän som finns men som i regel inte används av svenska användare (jämför till exempel awdasdawd.com och cnn.com). De förstnämnda filtreras bort när de returnerar NXDOMAIN medan de sistnämnda är utom kontroll. Det är alltså inte möjligt att säkert säga att samtliga undersökta domäner används i Sverige. Att en påhittad adress sammanfaller med en giltig antas dock vara sällsynt, resultatet bör därför påverkas endast i liten utsträckning.

Som nämnts under rubriken *Hur SPF fungerar* på sidan 4 krävs att båda parter är delaktiga i SPF för att det ska göra nytta under en transaktion. Avsändaren måste ha publicerat SPF-regler på förhand och mottagaren måste kontrollera dessa när e-post tas emot. Denna undersökning har endast kontrollerat hur många som har publicerat regler. Att mäta antalet e-postservrar som kontrollerar SPF är svårare, av flera anledningar. Olika implementationer av e-postservrar ger olika felmeddelanden vid olika tidpunkter under en transaktion om den stoppas på grund av ett brott mot publicerade SPF-regler. Dessutom kan e-postservrar ge felmeddelanden som kan misstas för att bero på SPF trots att de uppstått av en annan anledning. Problemet går dock att lösa genom att bevaka uppslagningar som görs mot en egen DNS-server under en transaktion. Detta skulle däremot kräva att ett fullständigt meddelande skickas för varje domän och det skulle kunna klassas som "unsolicited bulk mail" det vill säga spam. Något som gärna undviks. Resultatet från en sådan mätning skulle emellertid vara av intresse.

Förfalskad e-post

Faktumet att e-postavsändarens adress går att förfalska har varit känt sedan SMTP:s barndom (RFC 821, den första formella definitionen, är från 1982). Protokollet designades primärt för att leverera meddelanden "tryggt" och "pålitligt", man kunde förstås omöjligt förutse hur populärt det skulle komma att bli. Hade man det så skulle protokollet förmodligen ha sett något annorlunda ut.

Amerikanska CERT skriver i ett dokument⁷ från andra halvan av 90-talet att e-postbedrägerier ofta kan syfta till att lura någon att släppa ifrån sig känslig information. Phishing-attacker (som var välkänt redan då) handlar om precis detta. Phishing börjar ofta med ett förfalskat e-postmeddelande som under någon falsk förevändning uppmanar användaren att lämna ifrån sig känslig information. Phishing riktar sig i regel mot ett stort antal användare i taget och framförallt är det personer med liten datorvana⁸ som drabbas. Vad som på senare tid har fått större utrymme i allmän media är riktade attacker som vänder sig mot enskilda personer i en organisation; både i Sverige⁹ och i utlandet¹⁰. Ett exempel på hur systematiskt detta utnyttjats kom nyligen fram i en rapport¹¹ där man konstaterade att 103 länder utsatts för cyberspionage.

⁷ http://www.cert.org/tech_tips/email_spoofing.html

⁸ Det är därför rimligt att anta att SPF skulle ha en begränsad effekt på phishing-attacker; en användare som villigt följer en länk till <http://www.foretag.se.kdplwjsy.cn/> kommer inte att reagera över en misstänkt avsändaradress.

⁹ <http://www.idg.se/2.1085/1.208101/riktade-e-postattacker-mot-svenska-chefer>

¹⁰ http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

¹¹ <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>

Korrelation mellan bolagets storlek och SPF

Korrelationen mellan storlek och SPF är tydlig; bolag på OMX Large Cap använder SPF i större utsträckning än andra. På samma sätt har SPF större utbredning på Mid Cap än på Small Cap även om skillnaden är avsevärt mindre. Vårt resultat stämmer även väl överens med tidigare undersökningar på Fortune 1000 företag där andelen funnits ännu högre.

Resultatet kan upplevas som något motsägelsefullt. Exempelvis borde det vara enklare för ett mindre bolag att skriva SPF-regler då deras e-postsystem sannolikt är mindre invecklat. Å andra sidan har stora företag större system och har därmed ett större behov av specialiserad kompetens, både internt och genom konsulter. I kombination med att man även har en större genomströmning på personal talar för att det skulle vara mer troligt att SPF används. Detta eftersom om man väl en gång infört SPF behöver man aldrig göra det igen, så sammantaget talar fler personer och mer specialiserad kompetens för en större sannolikhet att situationen uppmärksammas och åtgärdas.

Ytterligare en hjälpare faktor för att införa SPF är att bolag på Large Cap i större utsträckning kommit i kontakt med regelverk så som Sarbanes-Oxley Act (SOX). Genom dessa regelverk kan det tillkomma struktur och kontroll i bolaget, vilket förenklar införandet av SPF. Har ett bolag dessutom infört system för Data Leakage Prevention (DLP) där man söker igenom all utgående e-post har man minskat tröskeln för införande till en mycket låg nivå.

Användningen av SPF

Generellt verkar användningsgraden ligga mellan tio och trettio procent i Sverige. Hur kommer det sig att SPF inte har nått större framgångar? SPF är ingen produkt som måste köpas och det kräver ingen licens för att använda. Det är ett öppet protokoll som vem som helst får utnyttja helt fritt. Varför är siffrorna så låga? Nedan presenteras ett antal teorier.

Man måste vara två

Som redan har behandlats i *Hur SPF fungerar* på sidan 4 kräver SPF att både avsändare och mottagare är delaktiga i protokollet för att resultat skall uppnås. Alltså, om alla utom du har publicerat regler har du stort utbyte av att kontrollera dessa. På samma sätt har du ingen nytta av att publicera regler för din domän om ingen annan kontrollerar dessa. Om bara var tionde domän har regler publicerade så kanske nyttan av att kontrollera alla domäner inte anses väga upp mot arbetet att införa kontrollen och ta eventuella problem som kan uppstå. Om många då avstår från att kontrollera de regler som bara är uppsatta för var tionde domän finns inte heller något större incitament för att publicera regler. Detta i synnerhet då publikation av regler i vissa fall kan vara komplex.

Stora miljöer

Ett bolag som endast har en utgående e-postserver eller flera servrar som använder samma IP-adress kan använda sig av en enkel regel i SPF. Organisationer med stora invecklade system för e-posthantering där e-post skickas från många olika platser med olika domännamn har ett svårare arbete framför sig. SPF definierar dock många direktiv som syftar till att underlätta sådana

organisationers arbete. Detta strider dock till viss del mot resultatet att större bolag (Large Cap) använder SPF i större utsträckning än små (Small Cap). Detta tas upp i sektionen om *Korrelation mellan bolagets storlek och SPF* på sidan 11. Hur dessa direktiv är utformade ligger utanför denna rapports omfång.

E-post är det viktigaste vi har

Under förberedelserna inför de penetrationstester som genomförs av HPS kommer det ofta fram att kunder anser sig vara särskilt beroende av att dess e-posttrafik fungerar tillfredsställande och att den inte får störas. Detta kan förstås innebära att det är otäckt att införa ett protokoll som syftar till att begränsa hur e-post får skickas. Dock, precis som sades i föregående sektion om *Stora miljöer*, så har SPF direktiv som möjliggör ett "mjukt" införande av reglerna som kan användas under en testperiod. Instrumentet kan trots detta upplevas trubbigt eftersom avsändaren har svårt att få direkt feedback om hur mottagaren hanterar skickad e-post.

Skyddar mot attacker som är förhållandevis okända

Även om e-postbedrägerier förekommer och rapporteras om i media, är det enligt vår erfarenhet okänt för de flesta människor. Jämför med exempelvis spam som är så vanligt förekommande att alla som har e-post har fått stifta bekantskap med det. Konsekvenserna är dessutom lätta att värdera i form av den tid det tar att rensa. Kontrasten mot riktade angrepp med e-postbedrägerier är stor – man upptäcker inte nödvändigtvis de angrepp som faktiskt sker, och konsekvenserna är svåra att bedöma.

Slutsats

Slutsatserna från undersökningen kan sammanfattas i tre punkter:

- En klar majoritet av bolag på svenska OMX-börsen riskerar att utnyttjas vid e-postbedrägerier.
- Stora bolag är bättre än små bolag på att skydda sig.
- Svenska bolag ligger flera år efter Fortune 1000-bolagen.

High Performance Systems

Författarna Carl-Johan Bostorp och Stefan Pettersson är specialister på IT-säkerhet på High Performance Systems AB i Solna.

High Performance Systems AB (HPS) är ett IT-konsultföretag som levererar hög driftsäkerhet till sina kunders IT-miljöer. Affärsidén kombinerar två kunskapsområden när en effektiv IT-lösning definieras; driftsäkerhet och informationssäkerhet.