E-Posta Sunucularında Adım Adım SPAM ve Spoofing Denetiminin Gerçekleştirilmesi

Hem kurumsal hem de gündelik hayatın vazgeçilmezlerinden biri olan e-postalar günümüzde iletişim için yaygın kullanılan araçlardan biri halindedir. Özellikle iş hayatında birçok kritik noktada görev yapan e-posta hesapları ile yeterli düzeyde güvenlik önlemi alınmazsa sosyal mühendislik saldırıları düzenlemek oldukça kolaydır. Günümüzde eposta sunucularında kullanılan teknoloji **SMTP** (*Simple Mail Transfer Protocol*) protokolü ve bu protokol üzerinegeliştirilmiş türevlerdir..

SMTP protokolü adından da anlaşılabileceği gibi temel e-posta alış veriş işlemlerini gerçekleştirmek için hazırlanmış bir protokoldür. Protokol ilk tasarlandığı 1982 yılında güvenlik gereksinimleri düşük ancak kullanılabilirliği yüksek bir prototip olarak hayat bulmuştur. Teknolojinin hızlı ilerlemesi ve güvenlik gereksinimlerinin artması **SMTP** protokolünün kullanımının da değişen şartlara ayak uydurması sonucunu doğurmuştur. Her ne kadar protokol temel aldığı yapıdan çok sapma göstermese de, protokolü güvenli hale getirmek için uygulanan yöntemler, e-posta trafiğinin daha güvenli şartlar altında gerçekleştirilmesine katkıda bulunmuştur..

SMTP servislerini protokolün ilk tasarlandığı 1982 yılındaki hali ve temel özellikleriyle kullanmak, aradan geçen onlarca yılda oluşan saldırı yöntemlerinin hepsinin riskini kabul etmek demektir. Temelinde e-posta transferinin gerçekleşmesi için değişmemiş olan protokol, ek güvenlik önlemleri ile konfigürasyon sıkılaştırma "*Configuration Hardenning*" işlemlerinden geçmezse birçok sosyal mühendislik saldırı türüne zafiyet barındırmaktadır.

Güvenlik önlemi alınmamış **SMTP** servislerinde bir başkası gibi e-posta yollamak mümkündür. Bir başkası gibi e-posta yollamak dışında SPAM (*istenmeyen*) e-posta yollanması ve servis engelleme saldırıları da bu kapsama girebilmektedir. Günümüzdeki güvenliği zayıf **SMTP** servislerinin yaygınlığı söz konusu olduğunda bunun uzman gözlemine dayalı nitel oranının Türkiye'deki kurumlar için en az %**60-70** olduğunu söyleyebilmek olasıdır.

Bir **SMTP** servisinin temel görevlerinde güvenliği ne kadar sağlayabildiğini görmek adına **Black Box** (*kara kutu*) birkaç test uygulamak yeterli olacaktır. Bu testler sonucunda **SMTP** servisinin ne tarz saldırılarda kullanılabileceği hakkında fikir sahibi olunabilir.

Sosyal mühendislik (kimlik taklit etme, oltalama, vb.) saldırıları ve SPAM mesajlarına karşı SMTP servisinin güvenliği aşağıdaki yöntemlerle test edilebilir.

Verilecek örnekler için kullanılacak adresler şu şekildedir:

- Kurban olarak, "*example*" kurumunda çalışan (*kurban@example.com.tr*) adresi seçilecektir

Saldırgan ise iki farklı gruptan seçilecektir,

- Birinci grup İnternet kanalıyla gelen saldırgan (*hacker@pwc.com*, gokhan.muharremoglu@pwc.com
- İkinci grup kurum içi çalışan/saldırgan (*gokhan.muharremoglu@example.com.tr*, hacker@example.com.tr)

Kimligi taklit edilecek kişi ise kurum içinden seçilecektir,

- Saldırıda kimliği taklit edilecek adres (*yonetici@example.com.tr*) olacaktır.

Senaryolarda e-posta sunucusunun İnternet veya Intranet'e hizmet veriyor olmasından bağımsız durumlar irdelenecektir.

SMTP servislerinin **SPAM** mesajlarına ve kimlik taklitçiliğine (*Spoofing*) karşı süseptibilitesi incelenirken aşağıdaki senaryolar kontrol edilmelidir:

1. Kurum içinden kurum içine yollanan e-postalar (*a@kurum → SMTP → b@kurum*)
2. Kurum içinden kurum dışına yollanan e-postalar (*a@kurum → SMTP → b@internet*)
3. Kurum dışından kurum içine yollanan e-postalar (*a@internet → SMTP → b@kurum*)
4. Kurum dışından kurum dışına yollanan e-postalar (*a@internet → SMTP → b@internet*)

Burada kurum kelimesi ile ifade edilmek istenen olgunun teknik karşılığı Local (yerel e-posta), İnternet ile ifade edilmek istenen olgunun teknik anlamdaki karşılığı ise External (dış e-posta) terimidir. Yukarıdaki maddelerde bahsedilen senaryolar ise teknik olarak **SMTP** servisi içindeki "*Relay*" ve "*Authentication*" ayarlarının denetleneceği durumlara tekabül eder.

Relay kelimesi Türkçe karşılığı ile aktarım yapmak anlamındadır. Örnek olarak, Open Relay hizmet verecek şekilde ayarlanmış (senaryo 4) bir **SMTP** servisi kendisine dış e-posta adresinden gelen bir mesajı Proxy (*vekil*) sunucusu gibi başka bir **SMTP** sunucusuna aktarır. Kendisine gelen e-postayı yerel bir posta kutusuna iletmez.

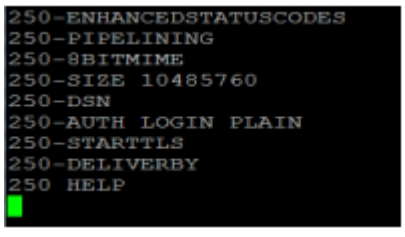
SMTP servisi doğası gereğince 1 ve 2 numaralı senaryo maddelerinde Authentication (*kimlik doğrulama*) işlemi yapabilir iken, 3 ve 4 numaralı senaryo maddelerinde bunu gerçekleştiremez. **SMTP** servisinin görevi kendine iletilen mesajı bir posta kutusuna veya başka bir e-posta sunucusuna iletmektir. Bu posta kutusu kendi yerel sunucusuna ait bir posta kutusu olduğunda gelen mesajın sahibinin kimlik doğrulaması için yerel posta kutusu hesabı kimlik bilgileri ile karşılaştırma yapabilir. Ancak mesajı yollayan bir dış hesap olduğunda kimlik kontrolü yapmak ancak çeşitli ek yöntemlerle sağlanabilir. Bu yöntemler 1982 **SMTP** tasarımında olmayan yöntemlerdir ve günümüzde her **SMTP** servisinde bu **DNS** tabanlı özellikler kullanılmadığından "*Junk*" veya "*Spam*" adı altında işaretlenen doğrulanmamış veya repütasyonu düşük mailler oluşturularak e-postalar ayrı bir klasörde tutulurlar.

SMTP servisinin manuel güvenlik denetimi:

Kurumun **SMTP** servisinin hizmet verdiği **SMTP** sunucusunun adresine Telnet ile bağlantı gerçekleştirir. Varsayılan **SMTP** Port'u *25*'dir. Bazı servisler *587* Port'unu da erişime açmaktadırlar. Bu adımdan sonra komutlar interaktif bir şekilde girilerek **SMTP** servisi ile konuşulur.

İlk test **SMTP** servisinin *1982* modelinin üstüne inşa edilerek oluşturulmuş **ESMTP** (*Enchanced SMTP*) komutlarından **EHLO** (*Extended HELO*) komutunun girilmesidir. Bu komut **SMTP** servisinin şifreli bağlantı kullanıp kullanmadığı veya Authentication gereksiniminin bulunup bulunmadığı gibi konular hakkında bilgiler verir.

Yandaki şekilde düz metin Authentication desteği veren ancak şifreli kimlik bilgisi transferi desteği vermeyen **SMTP** servis cevabı görülmektedir:



SMTP üzerindeki trafik **STRTTLS** komutuyla şifrelenebilmektedir. Bu desteğin olmadığı servisler ağ katmanındaki trafik dinleme saldırına karşı korumasızdırlar. **STARTTLS** komutu sayesinde düz metin olarak başlatılan trafik, şifreli olarak devam edebilme şansı bulur. **SMTP** servisine ait trafiğin tamamiyle SSL şifreleme üzerinden verilebileceği durumlar da mevcuttur.

Senaryolar bazında adım adım güvenlik denetiminin gerçekleştirilmesi:

1. ***Kurum içinden kurum içine yollanan e-postalar (a@kurum → SMTP → b@kurum)***

Aşağıdaki örnekte "*yonetici@example.com.tr*" adresinden yollanan e-posta adresinin hiçbir kimlik bilgisi sorulmadan kuyruğa alındığı görülebilmektedir.

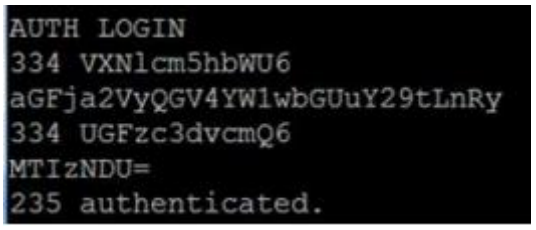
Yönetici kimliğini bu sayede taklit eden bir saldırgan kurban seçtiği kişiye e-posta göndermeyi başarabilir.

Bu senaryoda kimlik bilgisinin sorulması konusu söz konusu olduğunda karşılaşılması gereken ekranın aşağıdaki gibi olması gereklidir.

SMTP Authentication saldırı yüzeyini azaltmaya yardımcı olmaktadır. Ancak, kimlik taklitçiliğinde kullanılan saldırı yöntemlerini tek başına engelleyememektedir

SMTP Authentication (*kimlik doğrulama*) yapılmasının şart koşulduğu durumlarda dahi var olmayan posta kutularından geliyor gibi gösterilen e-postalar atmak mümkün olmaktadır. Aşağıdaki ekran var olan bir posta kutusunun kullanılarak, var olmayan bir posta kutusundan geliyor gibi gösterilecek bir e-postanın nasıl gönderilebileceğini göstermektedir

Kimlik doğrulama işlemi adımları **Base64** ile Encode edilmiş içeriği barındıracaktır



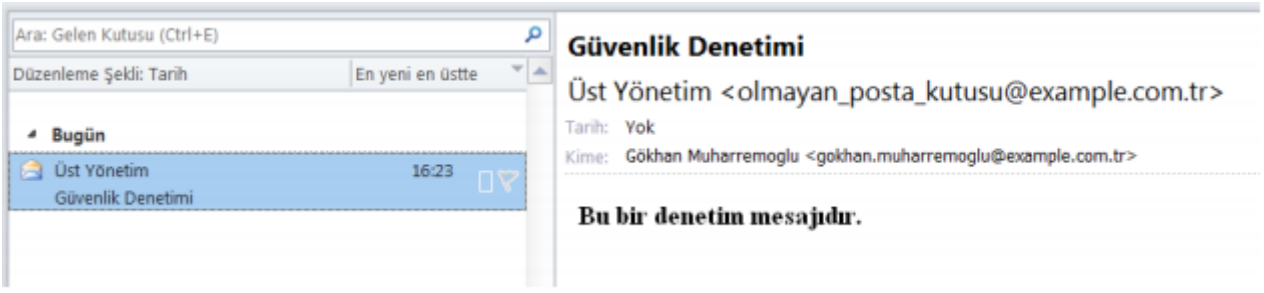
E-posta mesajının yollanması:

```
220 EXAMPLE.COM.TR KURUMSAL SMTP SERVISI
HELO EXAMPLE.COM.TR
502 Use HELO/EHLO first.
HELO EXAMPLE.COM.TR
250 Hello.
AUTH LOGIN
334 VXNlcm5hbWU6
aGFja2VyQGV4YW1wbGUuY29tLnRy
334 UGFzc3dvcmQ6
MTIzNDU=
235 authenticated.
MAIL FROM: hacker@example.com.tr
250 OK
RCPT TO: gokhan.muharremoglu@example.com.tr
250 OK
DATA
354 OK, send.
From: "Üst Yönetim" <olmayan_posta_kutusu@example.com.tr>
To: "Gökhan Muharremoglu <gokhan.muharremoglu@example.com.tr>
Subject: Güvenlik Denetimi
Mime-Version: 1.0;
Content-Type: text/html; charset="ISO-8859-9";
Content-Transfer-Encoding: 7bit;

<html>
<body>
<b>Bu bir denetim mesajıdır.</b>
</body>
</html>
.
250 Queued (18.798 seconds)
```

Var olan posta kutusu ”*hacker@example.com.tr*” adresi kullanılarak, var olmayan posta kutusu “*olmayan_posta_kutusu@example.com.tr*” adresinden geliyor gibi e-posta yollanmıştır.

E-posta mesajının “*Gelen Kutusu*” içindeki görüntüsü:



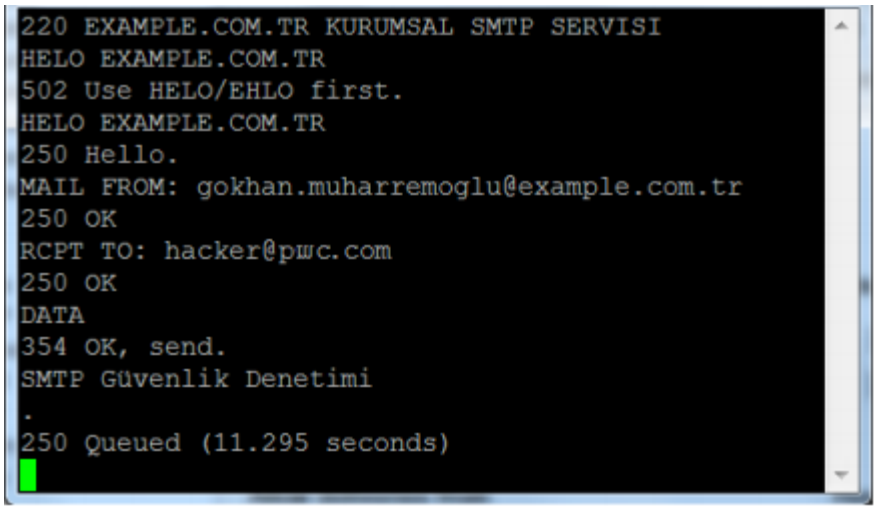
Posta kutularına iletilen mesajlar ile kurum içinde oltalama yapmak amacıyla sosyal mühendislik senaryoları uygulanabilir veya kurum çalışanları arasında tartışmalara neden olabilecek asılsız e-postalar kurum içine yollanabilir. Özellikle toplu e-posta gönderiminin yapıldığı ortak hesaplara yollanan e-posta adresleri seçilerek bu mesajlar kurum içine tek bir seferde yollanabilir.

Kullanılan ağ ve sistem tasarımına uygun olarak hazırlanacak bir sosyal mühendislik çalışmasında senaryoları çeşitlendirmek mümkün olacaktır.

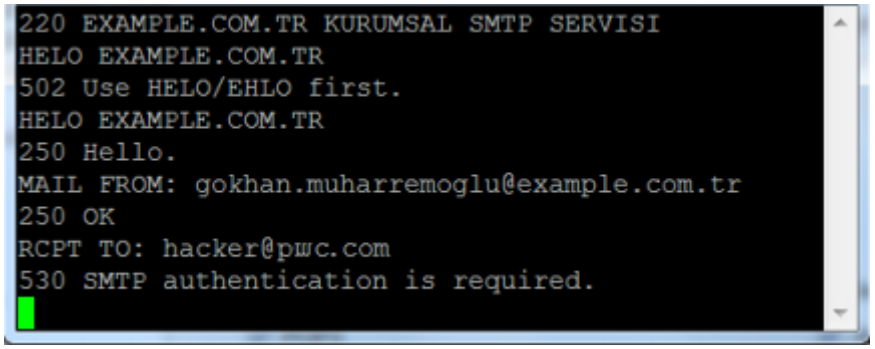
2. ***Kurum içinden kurum dışına yollanan e-postalar (a@kurum → SMTP → b@internet)***

Kurum içinden dışarıya yollanan e-postalar için **SMTP** Authentication kullanılmaması, kurum içinden birinin bir başkasının kimliğini taklit etmesine yarayabileceği gibi, **SMTP** servisinin İnternet'e de hizmet veriyor olması durumunda İnternet üzerindeki herhangi birinin kurum içinden geliyormuş gibi e-postalar atabilmesine de neden olabilir.

Aşağıdaki ekran görüntüsünde İnternet üzerinden gelen ve kurum içi bir çalışandan geliyor izlenimi uyandıran bir epostanın **SMTP** servisi tarafından kabul edildiği ve dağıtım kuyruğuna alındığı görülmektedir.



Bu senaryoda kimlik bilgisinin sorulması konusu söz konusu olduğunda karşılaşılması gereken ekranın aşağıdaki gibi olması gereklidir.



Kurum SMTP Sunucusunun SPAM Aracı Olarak Kullanılması

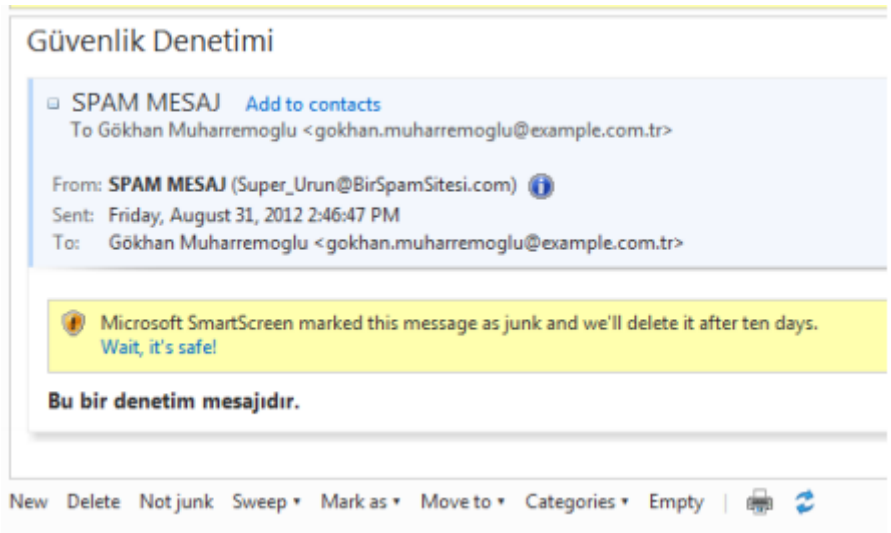
Internet'e de açık olan e-posta sunucuları için **SMTP** servis konfigürasyonun bilinçli bir şekilde yapılmış ve kullanım şartlarına uygun bir güvenlik anlayışı ile uygulanmış olması gerekmektedir. Aksi takdirde kurumun **SMTP** servisi **SPAM** aracı olarak kullanılabilir. **SPAM** aracı olarak kullanılan **SMTP** servisinden yollanan e-postalar 2. Senaryo dâhilinde karşı tarafa kurum dışından geliyor gibi gösterilerek de yollanabilir. Bunun için 1. senaryoda anlatılan olmayan posta kutusundan geliyormuş gibi gönderilen e-posta yönteminin bu senaryo için de gerçekleştirilmesi gereklidir.

Aşağıdaki örnekte "*kurban@example.com.tr*" e-posta adresi kullanarak "*Super_Urun@BirSpamSite.com*" adresinden geliyormuş gibi gösterilen bir e-posta, "*gokhan.muharremoglu@pwc.com*" adresine gönderilirken, aynı zamanda gönderilmiş olan adres "*gokhan.muharremoglu@example.com.tr*" gibi gösterilmiştir.

```
220 EXAMPLE.COM.TR KURUMSAL SMTP SERVISI
HELO EXAMPLE.COM.TR
502 Use HELO/EHLO first.
HELO EXAMPLE.COM.TR
250 Hello.
MAIL FROM: kurban@example.com.tr
250 OK
RCPT TO: gokhan.muharremoglu@pwc.com
250 OK
DATA
354 OK, send.
From: "SPAM MESAJ" <Super_Urun@BirSpamSitesi.com>
To: "Gökhan Muharremoglu <gokhan.muharremoglu@example.com.tr
>
Subject: Güvenlik Denetimi
Mime-Version: 1.0;
Content-Type: text/html; charset="ISO-8859-9";
Content-Transfer-Encoding: 7bit;

<html>
<body>
<b>Bu bir denetim mesajıdır.</b>
</body>
</html>
.
250 Queued (72.306 seconds)
```

Teslim alınan mesajın e-posta kutusundaki görüntüsü:



Bu durum bir süre sonra kuruma ait **SMTP** sunucusu **IP** adreslerinin kara listelere girmesine ve kurum e-postalarının **SPAM** olarak işaretlenmesine neden olabilir.

3. Kurum dışından kurum içine yollanan e-postalar (a@internet → SMTP → b@kurum)

Bu senaryodaki durum e-posta kimlik taklitçiliğinden (*Spoofing*) en çok etkilenen öğeleri bir arada barındırmaktadır. E-postayı gönderen tarafın kimlik bilgilerinin **SMTP** kimlik doğrulama ile doğrudan tespit edilmesi olanaklı değildir. Çünkü gönderen tarafın e-posta kutusuna ait kimlik bilgileri, mesajın teslim edildiği tarafta bulunmamaktadır.

Bu durumdan doğacak suiistimalleri bertaraf etmek ve e-postayı gönderen tarafın kimliğini onaylamak için **SMTP** protokolü üzerine ek güvenlik önlemleri geliştirilmiştir. Bu önlemlerde hedeflenen amaca ulaşmak için taklit (*Spoof*) edilemeyen değerlerden yola çıkılmaktadır. E-postanın gönderildiği IP adresinin ve e-postanın "@" işaretinden sonraki Domain kısmına ait DNS bilgilerinin sorgulanarak, gönderen tarafın değerleri ile bütünlük karşılaştırılması yapılması bunlardan biridir.

SPAM ve E-posta taklitçiliğini (*Spoofing*) engellemeye yönelik geliştirilmiş ek önlemlerden başlıcaları şu şekildedir:

A. SPF (Sender Policy Framework) - Gönderen Teyit Politikası

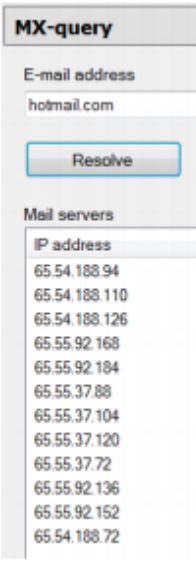
Gönderen tarafın gönderdiğini iddia ettiği Domain'e ait **DNS** bilgilerindeki bir **TEXT** kaydı içinde o Domain adına eposta göndermeye yetkilendirilmiş **SMTP** servis sunucu bilgileri tutulur. Bu şekilde gönderen tarafın IP adresinin gerçekte o Domain'e ait yetkili bir IP adresi olup olmadığının tespiti yapılmış olur. E-posta mesajını gönderen sunucu, Domain **DNS** kayıtlarında listelenmiş sunuculardan biri değilse mesaj **SPAM** olarak değerlendirilir.

Aşağıda "*pwc.com*" Domain adı için **DNS** bilgilerinde listelenmiş olan **SPF** bilgisini veren **TEXT** (TXT) kaydı görünmektir

SMTP protokolü adından da anlaşılabileceği gibi temel e-posta alış veriş işlemlerini gerçekleştirmek için hazırlanmış bir protokoldür. Protokol ilk tasarlandığı 1982 yılında güvenlik gereksinimleri düşük ancak kullanılabilirliği yüksek bir prototip olarak hayat bulmuştur. Teknolojinin hızlı ilerlemesi ve güvenlik gereksinimlerinin artması **SMTP** protokolünün kullanımının da değişen şartlara ayak uydurması sonucunu doğurmuştur. Her ne kadar protokol temel aldığı yapıdan çok sapma göstermese de, protokolü güvenli hale getirmek için uygulanan yöntemler, e-posta trafiğinin daha güvenli şartlar altında gerçekleştirilmesine katkıda bulunmuştur..

Answer records

pwc.com	A	216.34.181.97	3600s
pwc.com	MX	preference: 0	3600s
		exchange: faad44f2dcb945aac2b7fcbdecc5ef.pamx1.hotmail.com	
pwc.com	NS	ns33.domaincontrol.com	3600s
pwc.com	NS	ns34.domaincontrol.com	3600s
pwc.com	TXT	v=spf1 include:hotmail.com ~all	3600s
pwc.com	TXT	v=msv1 t=faad44f2dcb945aac2b7fcbdecc5ef	3600s



Yukarıdaki SPF kaydı içindeki geçen değerlerin anlamları şu şekildedir:

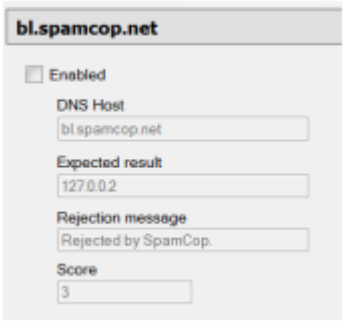
- "*v=spf1*" → SPF sürüm bilgisi **v.1.0**'dır.
- "*include:hotmail.com ~all*" → Yetkilendirilmiş sunucular olan (*Hotmail.com*)sunucuları dışında bütün sunucular (*~all*) bu Domain'den e-posta yollamaya yetkili değildir

Yetkilendirilmiş sunucular bir **MX** sorgusu ile listelenebilir →

TEXT (*TXT*) kaydı içinde görünen değerlerin yorumlanması için kullanılan söz dizimindeki işaretler aşağıdaki anlamları taşımaktadırlar:

İşaret	İşlem	Açıklama	Eylem
"+"	Pass	Sunucu izin verilenler listesindedir.	İzin ver
"-"	Fail	Sunucu izin verilmeyenler listesindedir.	Engelle
"~"	SoftFail	Mesaj e-posta kutusuna iletilecektir; ama durumu SPAM olarak değerlendirilecektir.	İzin ver
"?"	Neutral	SPF kaydı sunucu durumunu değerlendirmeye almayacaktır.	İzin ver

Kuruma ait e-posta adreslerinin taklit edilmesinin önüne geçilebilmesi için kuruma ait e-posta Domain'in **DNS** kayıtlarına **SPF** kayıtlarının da eklenmesi gereklidir. **SPF** kaydı kontrolü yapan e-posta sunucularına taklit edilmiş eposta yollanmasının önüne bu şekilde geçilebilir. Ancak, kurum **DNS** kaydı bilgilerini girmiş olsa bile **SPF** kontrolü yapmayan e-posta sunucuları taklit edilmiş e-posta adreslerini **SPF** yoluyla ayırt edemez.



B. DNS-based Blackhole List (DNSBL) - DNS Kara Listeleri

DNS-based Blackhole List (*DNSBL*) veya Real-time Blackhole List (*RBL*) olarak da bilinir. Dünya çapında **SPAM** yaptığı bilinen IP adreslerine ait bir listenin **SMTP** sunucusu tarafından engellenmesi ile **SPAM** mesajlarının önüne geçilmesi hedeflenir. Ancak bu yöntem, yukarıda 2. Senaryo maddesindeki "*Kurum **SMTP** Sunucusunun **SPAM** Aracı Olarak Kullanılması*" örneğinde de anlatıldığı üzere **SPAM** aracı olarak kullanılmış eposta sunucularının da **SPAM** olarak değerlendirilmesine neden olabilmektedir.

C. SURBL – URL Kara Listesi

SPAM yaptığı bilinen Web sitelerine ait **URL** (*adres*) linklerinin içinde bulunduğu e-posta mesajlarının **SPAM** olarak değerlendirilmesini sağlayan başka bir kara liste çeşididir

D. Greylisting - Gri Liste Yöntemi

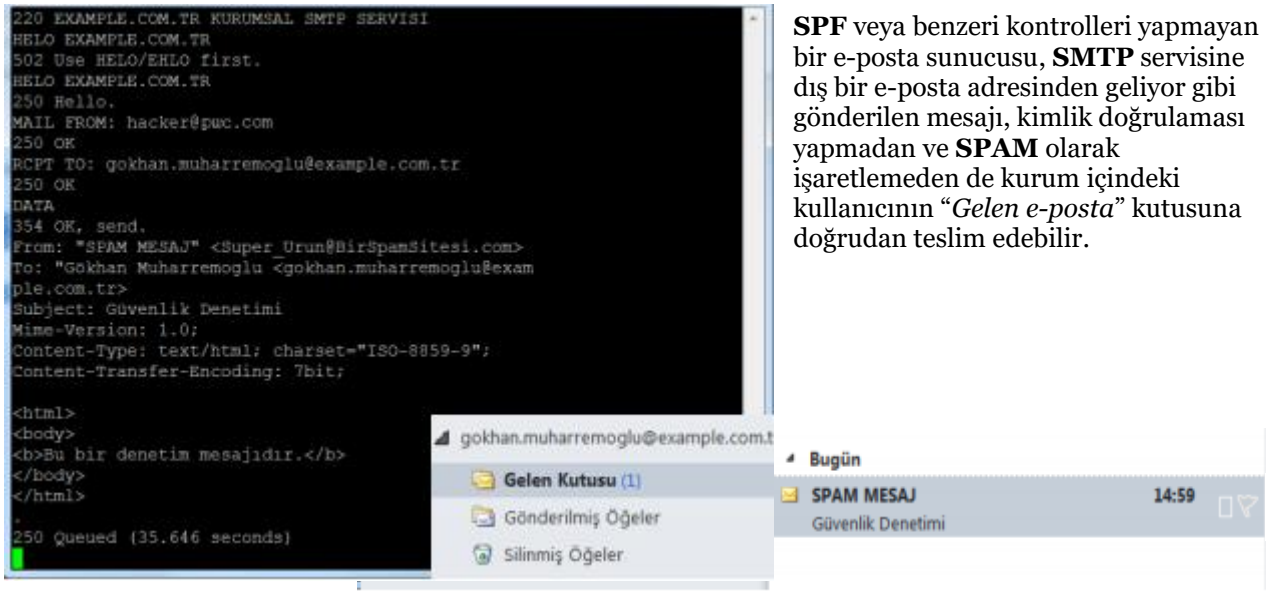
Bu yöntemde sunucu ile ilk defa konuşmaya başlayan bir IP adresinin gönderdiği e-posta mesajı doğrudan reddedilir ve gönderene daha sonra tekrar denemesi söylenir. IP adresi, gönderen e-posta adresi ve alıcı e-posta adresi olmak üzere 3 adet öğe kayıt altına alınır. Bu 3 öğe ile tekrar e-posta yollanmak istenirse, e-posta sunucusu isteği kabul eder ve mesajı gerekli adrese ulaştırır.

E. DKIM (Domain Keys Identified Mail) - Alan Adı Anahtarıyla E-Posta Kimlik Doğrulaması

Gönderilen her e-posta mesajının kriptografik olarak açık anahtar (*Public Key*) sistemiyle imzalanmasına dayalı bir yöntemdir. Gönderen Private Key kullanarak mesajı imzalar. Aynı zamanda imzalanmış mesajın doğrulanması için gerekli olan Public Key bilgisini ise **DNS** kayıtları üzerinden yayına sunar. Mesajı alan e-posta sunucusu, aldığı mesajı Public Key ile işleme sokar ve mesajın imzasını kontrol eder. Eğer mesaj için oluşturulmuş kriptografik özet, Public Key ile elde edilen özetle eşleşiyorsa, bu mesaj kaynağı onaylanmış olarak işaretlenir.

F. IP Adres Aralığı Sınırlandırılması

E-posta sunucusuna mesaj iletebilecek IP adres bloklarının önceden belirlenmesi ile **SPAM** ve Spoofing konularında ek önlemler alınabilir. Dinamik **ADSL** IP adresleri gibi aralıkların sunucuya erişemeyecek şekilde belirlenmesi bu önleme bir örnek olarak gösterilebilir. Benzer şekilde İnternet'e bakan bir yüzü olan kurum e-posta sunucularında içerideki ağa ait IP adreslerinin belirlenip, bu adreslere göre kurallar tanımlanması kullanılabilirlik-güvenlik dengesini verimli bir noktaya çekecektir



SPF veya benzeri kontrolleri yapmayan bir e-posta sunucusu, **SMTP** servisine dış bir e-posta adresinden geliyor gibi gönderilen mesajı, kimlik doğrulaması yapmadan ve **SPAM** olarak işaretlemeden de kurum içindeki kullanıcının "*Gelen e-posta*" kutusuna doğrudan teslim edebilir.

4. *Kurum dışından kurum dışına yollanan e-postalar (a@internet → SMTP →b@internet)*

Kurum dışından olan bir e-posta adresi ile yine kurum dışından olan başka bir e-posta adresine kuruma ait e-posta sunucusunun kullanılarak mesaj gönderilmesi işlemidir. Teknik olarak "*Open Relay*" adıyla tabir edilen bu senaryoda kurumun e-posta sunucusu bir vekil sunucu (*Proxy*) gibi işlev görür ve kendisine verilen dış e-posta kutusu kaynaklı mesajı yerel bir posta kutusu yerine, bir dış e-posta kutusuna gönderir.Şekilde "*pwc.com*" Domain'ine ait dış bir eposta adresinden "*pwc.com*" Domain'ine ait başka bir e-posta kutusuna, "*Example.com.tr*" **SMTP** servisi aracılığı ile mesaj yollandığı görülmektedir.

Konfigürasyonu Open Relay yapılandırılmış bir e-posta sunucusu ile herhangi bir Domain'den herhangi bir Domain'e doğru yollanacak mesajlar oluşturmak ve bu mesajları kurumun sunucu IP adresi üzerinden göndermek mümkündür. Bu durumdaki sunucuların yukarıda izah edilen kara listelere hızlı bir şekilde girebileceği söylenebilir.

SPAM aracılığıyla reklam, propaganda yapmak isteyen saldırgan veya Worm gibi zararlı yazılımlar, bu tarz sunucuların varlığını İnternet üzerinden gerçekleştirdikleri keşiflerle otomatik olarak tespit etmektedirler. Belli başlı IP aralıklarının taranması ile keşfedilen Open Relay sunucular, başta **SPAM** olmak üzere çeşitli amaçlar için kullanılmaktadırlar. Bu amaçlardan bazıları adli bilişim konularına girebilecek türden olurken, bazıları da kurumun IP adreslerinin dünya çapında SPAM yapan sunucuların listelerine girmesiyle sonuçlanmaktadır.

İnternet'e de hizmet veren e-posta sunucuları için sıkılaştırılmamış konfigürasyon yapılandırmasının sadece kurum içine hizmet veren bir e-posta sunucusuna göre daha fazla risk içermesi olasıdır. Her kurum mevcut mimarisine bakarak riski nasıl yöneteceğine kendisi karar vermelidir. Bir zafiyet bir mimaride düşük önem taşırken, başka bir mimaride kritik önemdeki bir güvenlik sorununa işaret ediyor olabilir.

(Cyber, 25.10.2018)

Gökhan Muharremoğlu
Cyber Security, Senior Manager
Email: gokhan.muharremoglu@pwc.com