BGYS POLİTİKASI

Politika Numarası	PLTK-13
Politika Tanımı	Kötü Amaçlı Yazılıma Karşı Korunma Politikası
Amaç ve İlkeler	Bilgilerin ve diğer ilgili varlıkların kötü amaçlı yazılımlara karşı korunmasını sağlamaktır.
Sorumluluklar	**Bilgi İşlem Personeli:** Şüpheli veya potansiyel kötü amaçlı yazılım kullanımının engellenmesi amacıyla sistemin kurulması ve denetlenmesinden sorumludur. **Kullanıcılar**: Şüpheli veya potansiyel kötü amaçlı yazılım aktivitelerini derhal bilgi işlem birimine rapor etmekle sorumludur.
Sapma ve Özel Durumlar	Bu politikanın ihlali, disiplin önlemleri ve iş sürekliliğine bağlı kayıplara neden olabilir.

UYGULAMA

Kötü amaçlı yazılımların kullanımını engellemek veya tespit etmek amacıyla;

- Bilgisayar kurulumları sırasında standart kullanıcı hesapları tanımlanmalıdır. Bu hesaplar, kullanıcıların program kurulumu gibi yetkili işlemleri yapmasını engellemektedir. Böylelikle, bilgisayarlara yetkisiz yazılım yüklenmesinin önüne geçilmektedir.
- Bilgisayar sistemlerinde uç nokta güvenlik çözümleri kullanılmalıdır. Bu çözümler, bilgisayarların ve ağların korunmasına yönelik olarak yetkisiz yazılımları tespit ve müdahale etmektedir. Olumsuz durumlarda, bu çözümler otomatik olarak müdahale edebilmekte ve güvenliği sağlamaktadır.
- İzleme Takip programı yazılımları kullanılmalıdır. Bu yazılım, bilgisayar sistemlerini izleyerek olası tehditleri tespit etmekte ve bildirimler göndermektedir. Bir uygulama yüklenmek istendiğinde, sistem otomatik olarak bir bildirim e-postası göndererek yazılımın kurulduğunu bildirmekte ve ilgili cihaza hızlı müdahale imkanı sağlanmaktadır.
- Bu çalışmalar sayesinde, firma bünyesinde yetkisiz yazılımların kullanımıyla ilgili etkin bir denetim ve koruma sağlanmaktadır. Bilgisayar sistemlerinin güvenliği ön planda tutularak iş sürekliliği ve veri bütünlüğü sağlanmaktadır.

Bilinen veya şüphelenilen kötü amaçlı web sitelerinin kullanımını önleyen veya tespit etmek amacıyla;

- Siber Olaylara Müdahale Merkezi'nin (USOM) kara listesi takip edilmelidir. Bu liste, bilinen kötü amaçlı web sitelerini içermektedir. Şirketimiz, bu liste üzerinden erişimi engellenen siteleri belirleyerek kullanıcıların erişimini kısıtlamaktadır.
- Uç nokta güvenlik yazılımları kullanılmalıdır.
- Bilgi işlem personelleri tarafından şüpheli veya zararlı olarak belirlediği web sitelerini engellenenler listesine dahil edilmektedir. Bu sayede, şirket içinde tespit edilen zararlı web siteleri geniş bir kapsamda engellenebilmektedir. Bu kontroller sayesinde, şirketimizde çalışanların bilinmeyen ve zararlı web sitelerine erişimleri etkin bir şekilde engellenmekte ve kurumsal bilgi güvenliği sağlanmaktadır.
- Firewall cihazı üzerinde bulunan web filter modülü, şirketimizde web sitelerine erişimi daha da etkin bir şekilde kontrol etmemizi sağlamaktadır. Bu modül aracılığıyla, kullanıcıların belirli kategorilere veya özelliklere sahip web sitelerine erişimi kolayca engellenebilmektedir. Örneğin, sosyal medya siteleri, oyun siteleri veya belirli içerik kategorilerine sahip sitelere erişim kısıtlanabilmektedir.
- Firewall cihazı üzerindeki web filter modülü, ağ trafiğini izleyerek belirlenen politikalara uygun olarak web sitelerine erişimi kontrol eder. Bu sayede, şirket politikalarına uygun olmayan veya güvenlik riski taşıyan web sitelerine erişim engellenebilir.
- Ayrıca, bu modül sayesinde web siteleri üzerindeki kullanımı detaylı olarak izlenebilir ve raporlanabilir. Bu raporlar, hangi sitelere ne kadar süreyle erişildiği gibi bilgileri içerir ve şirketin bilgi güvenliği politikalarının etkinliğini değerlendirmede önemli bir rol oynar.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
25.04.2018	01/29.01.2024	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

BGYS POLİTİKASI

Kötü amaçlı yazılım tarafından yararlanılabilecek güvenlik açıklarının azaltılması amacıyla;

Firma bünyesinde bilgi güvenliği iş sürekliliğini sağlamak amacıyla düzenli olarak penetrasyon testleri yapılmalıdır. Bu testler sonucunda tespit edilen açıklar, hızla kapatılmalı ve ardından doğrulama testleri ile kontrol edilmelidir. Bununla birlikte, şirket içerisinde kullanılan uç nokta güvenlik çözümü ürünleri, bilgisayarlarda yüklü olan uygulamalardaki zafiyetler tespit edilerek raporlanmalıdır. Bu raporlar doğrultusunda bilgi işlem personelimiz, yazılım güncellemeleri yapmakta veya güvenlik açıklarını kapatabilmek için ilgili uygulamaları kaldırıp, güncel ve güvenilir yazılımları yeniden yüklemektedir. Bilgisayarlar, sürekli olarak uç nokta güvenlik yazılımları ile taranmalı ve korunmalıdır.

Firma bünyesinde, kritik iş süreçlerinin yürütülmesi genellikle manuel olarak gerçekleştirilmektedir. Bu süreçlerde, personel tarafından veriler elle kontrol edilmeli ve doğrulanmalıdır. Otomatik doğrulama sistemleri mevcut değildir ve süreçler genellikle insan denetimine dayanmaktadır.

Harici ağlardan veya bu ağlar aracılığıyla veya başka herhangi bir ortamdan dosya ve yazılım alınmasıyla ilgili risklere karşı koruyucu önlemler alınması amacıyla;

- Firma bünyesinde güvenlik duvarları kullanılarak harici ağlardan gelen dosya ve yazılımların trafiği kontrol edilir ve gerektiğinde engellenir. Güvenlik duvarları, istenmeyen ve potansiyel olarak zararlı içeriklere karşı koruma sağlar.
- Tüm gelen dosya ve yazılımlar, şirket içindeki bilgisayarlarda antivirüs ve kötü amaçlı yazılım taramasıyla taranır. Bu sayede zararlı içerikler tespit edilir ve izole edilir.
- Harici ağlardan gelen e-postalar, şüpheli veya zararlı içerikleri filtrelemek için e-posta güvenlik çözümleri kullanılarak kontrol edilir. Bu sayede kötü amaçlı dosya ve yazılımların şirket içine girmesi engellenir.
- Harici ağlardan veya başka ortamlardan yazılım ve dosya alımı yalnızca güvenilir kaynaklardan yapılır. Lisanslı ve güvenilir yazılım sağlayıcılarından alışveriş yapılır ve güvenlik sertifikalarıyla doğrulanmış dosyalar tercih edilir.

Bilgisayarları ve elektronik depolama ortamlarını kötü amaçlı yazılımlara karşı taramak ve bu yazılımları tespit ederek gidermek, bilgi güvenliğini sağlamak için kritik bir önlemdir. Bu amaçla aşağıdaki adımlar izlenir;

- Kötü amaçlı yazılım tespit ve giderme yazılımının yüklenmesi ve güncellenmesi
- Düzenli taramaların yapılması: Ağlar ve elektronik depolama ortamları, e-posta ve anlık mesajlaşma eklerinin ve indirmeleri, web sayfaları

Firma bünyesinde, bilgi güvenliği için derinlemesine savunma ilkeleri uygulanmaktadır. Öncelikle, ağ geçidinde kötü amaçlı yazılım tespiti için çeşitli önlemler alınmaktadır. E-posta, dosya aktarımı ve web gibi farklı uygulama protokolleri üzerinden gelen veriler kötü amaçlı yazılımlara karşı taranmakta ve gerekli önlemler alınmaktadır. Ayrıca, kullanıcı uç nokta cihazları ve sunucularda da kötü amaçlı yazılım tespiti yapılmakta ve gerekli önlemler alınmaktadır.

Saldırganların kötü amaçlı yazılım dağıtmak için kullandığı teknikler de göz önünde bulundurulmaktadır. Şirketimiz, dosyaların şifrelenmesi ve şifreleme protokollerinin incelenmesi gibi önlemlerle saldırganların kaçamak tekniklerini tespit etmekte ve önlem almaktadır.

Güvenlik yazılımlarını düzenli olarak güncelleyerek ve etkinleştirerek kötü amaçlı yazılımlara karşı koruma sağlanmaktadır. Antivirüs ve antimalware programları gibi koruma yazılımları, bilgisayarları ve ağ sistemlerini sürekli olarak tarayarak zararlı yazılımları tespit etmekte ve engellemektedir.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
25.04.2018	01/29.01.2024	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

Güvenlik duvarı ve ağ filtreleme önlemleri, firmamızın dış ağ trafiğini sürekli olarak izlemekte ve potansiyel zararlı trafiği engellemektedir. Bu önlemler, kötü amaçlı yazılımların dış kaynaklardan firma ağına girmesini önlemekte ve ağ güvenliğini artırmaktadır.

Firmamızda, düzenli olarak güvenlik incelemeleri ve denetimleri gerçekleştirerek sistemlerdeki güvenlik zayıf noktalarını tespit etmekte ve kapatmaktadır. Bu incelemeler, firma içi ağ ve sistemlerin güvenliğini sürekli olarak kontrol etmekte ve güvenlik önlemlerinin etkinliğini değerlendirmektedir.

Firmamız, personelin bilgi güvenliği konusunda eğitilmesi ve farkındalığının artırılması için düzenli eğitim ve bilinçlendirme programları düzenlemektedir. Personel, kötü amaçlı yazılımlara karşı nasıl korunacakları konusunda bilgilendirilmekte ve güvenlik politikalarına uygun davranışlar konusunda eğitilmektedir.

İşin gerekli doğrultusunda istisna onay yetkilerinin verilmesi gereken durumlarda kötü amaçlı yazılıma karşı korunma önlemleri dahilinde istisna onay yetkilendirmesi yapılabilmektedir.

Yıkıcı sonuçların ortaya çıkabileceği ortamların izole edilmesi kapsamında;

- Sistem izolasyonu sağlanmıştır. Bu doğrultuda, Kritik sistemler ve ağlar, fiziksel olarak ayrılmış odalarda barındırılmaktadır. Bu odalara sadece yetkili personel erişebilir ve erişim izinleri sıkı bir şekilde kontrol edilmektedir. Ağ segmentasyonu, işyeri ağını farklı bölümlere ayırarak, her bir segmentin kendi güvenlik duvarıyla izole edilmesini sağlamaktadır.
- Uygulama izolasyonu sağlanmıştır. Hassas uygulamalar, sanallaştırma teknolojisi kullanılarak ayrılmış sanal sunucularda çalıştırılmaktadır. Bu sayede, her uygulama birbirinden izole edilmiş ve bir uygulamadaki bir güvenlik açığı diğerlerini etkilemez hale getirilmiştir. Özellikle müşteri verilerini işleyen uygulamalar, ayrı güvenlik duvarları ile korunan sanal ortamlarda barındırılmaktadır.
- Hassas veriler, güvenli şifreleme yöntemleri kullanılarak korunmaktadır. Veritabanları ve depolama cihazları, güçlü şifreleme algoritmalarıyla korunarak, yetkisiz erişime karşı güven altına alınmıştır. Veri erişimi, sadece belirlenmiş yetkilendirilmiş personel tarafından gerçekleştirilebilir ve izlenir.
- Sunucu odaları ve veri merkezleri, yalnızca yetkilendirilmiş personelin erişimine açıktır. Bu alanlara giriş ve çıkışlar kayıt altına alınmakta ve izlenmektedir. Donanım ve depolama cihazları, güvenlik kameraları ve erişim kontrol sistemleri ile korunan güvenli bir ortamda saklanmaktadır.
- İzolasyon önlemleri, düzenli olarak test edilmekte ve değerlendirilmektedir. Güvenlik açıkları ve zayıf noktalar, periyodik olarak yapılan saldırı senaryoları üzerinde simülasyonlarla belirlenmekte ve giderilmektedir. İzolasyonun etkinliği, güvenlik ekibi tarafından sürekli olarak izlenmekte ve iyileştirme önlemleri alınmaktadır.

Tüm çalışanlar, kötü amaçlı yazılımların belirtileri, güvenli internet kullanımı ve e-posta güvenliği gibi konularda düzenli eğitimlere tabi tutulmalıdır. Bu eğitimler, Bilgi İşlem birimi tarafından planlanmakta ve düzenli aralıklarla gerçekleştirilmektedir.

Kurtarma Prosedürleri

Firma bünyesinde, olası kötü amaçlı yazılım saldırılarına karşı kurtarma planları geliştirmiştir. Bu planlar, saldırıların tespit edilmesi durumunda uygulanacak adımları ve kurtarma sürecini ayrıntılı olarak içermektedir. Kurtarma ekipleri, saldırı sonrası sistemi hızlı bir şekilde eski haline getirebilmek için gereken yazılım ve donanım yedeklerini hazır bulundurmakla sorumludur.

Sistem Güncellemeleri ve İyileştirmeleri

Sistem yöneticileri, kötü amaçlı yazılımlara karşı korumayı sürekli olarak güçlendirmek ve iyileştirmek için düzenli olarak sistem güncellemeleri ve yamalarını uygulamaktadır. Sistem yöneticileri, potansiyel riskleri değerlendirmek ve yeni tehditlere karşı önlem almak için sürekli olarak sistemleri ve güvenlik politikalarını gözden geçirmektedir.

Tüm kullanıcılara, kötü amaçlı yazılım bulaşmış e-postaların, dosyaların veya programların alınması, gönderilmesi veya yüklenmesinin belirtileri ve nasıl tanımlanacağı konusunda düzenli eğitimler sağlanmalıdır. Şirket içi iletişim kanalları aracılığıyla, kullanıcılara kötü amaçlı yazılımların nasıl yayıldığı, hangi tür e-postaların ve dosyaların potansiyel tehdit oluşturabileceği konusunda düzenli olarak bilgilendirici mesajlar ve duyurular yapılmalıdır.

Kullanıcılar, kötü amaçlı yazılım bulaşmış e-postaları, dosyaları veya programları fark ettiklerinde bunu derhal Bilgi İşlem birimine rapor etmeye teşvik edilir. Ayrıca, şüpheli etkinlikleri veya dosyaları raporlamak için kullanıcıların kolayca erişebileceği bir raporlama mekanizması bulunur.

Firma bünyesinde Kötü Amaçlı Yazılımlara Karşı Farkındalık ve Eğitim Süreçleri, çalışanların güvenlik konusundaki farkındalıklarını artırmak ve potansiyel tehditlere karşı daha hazır olmalarını sağlamak için etkin bir şekilde uygulanmaktadır.

Bilgi işlem birimi, yeni çıkan kötü amaçlı yazılımlar hakkında güncel bilgiye erişim sağlamak amacıyla güvenilir güvenlik haber kaynaklarına, posta listelerine, web sitelerine vb. abone olur ve düzenli olarak takip eder. Bu kaynaklar arasında siber güvenlik firmalarının resmi web siteleri, güvenlik haber siteleri ve güvenlik endüstrisi raporları bulunur. Toplanan bilgiler düzenli olarak analiz edilir ve değerlendirilir. Yeni çıkan kötü amaçlı yazılımların doğası, yayılma yöntemleri, etkileri ve karşı önlemler konusunda detaylı bir değerlendirme yapılır.

Kötü amaçlı yazılımla ilgili bilgiler, güvenilir ve saygın kaynaklardan elde edilir. Bu kaynaklar arasında güvenlik endüstrisi liderleri, siber güvenlik firmaları, kötü amaçlı yazılım tespit yazılımı tedarikçileri, siber güvenlik blogları ve güvenilir internet siteleri bulunur. Bilgi işlem birimi, kötü amaçlı yazılımla ilgili bilgileri çeşitli kaynaklardan derinlemesine araştırır. Özellikle, güvenilir internet siteleri, siber güvenlik blogları ve güvenlik tedarikçilerinin resmi bildirimleri incelenir.

Doğrulanmış bilgiler, ilgili departmanlar ve personel ile paylaşılır. Bilgilendirme süreci, şirket içindeki tüm ilgili kişilere güncel ve doğru bilgilerin aktarılmasını sağlar. Bu bilgiler, kötü amaçlı yazılımlara karşı korunma stratejilerinin güncellenmesi ve gerektiğinde acil önlemlerin alınması için kullanılır.