BGYS POLİTİKASI

Politika Numarası	PLTK-18
Politika Tanımı	Ağ Güvenliği Politikası
Amaç ve İlkeler	Şirket ağının güvenliğini sağlamak, yetkisiz erişimleri önlemek, hassas bilgilerin korunmasını sağlamak ve ağ kaynaklarının etkin bir şekilde yönetilmesini temin etmektir.
Sorumluluklar	**Bilgi İşlem Personeli:** Ağ güvenliğinin sağlanması amacıyla gerekli sistemin kurulması ve denetlenmesinden sorumludur.
Sapma ve Özel Durumlar	Bu politikanın ihlali, disiplin önlemleri ve iş sürekliliğine bağlı kayıplara neden olabilir.

UYGULAMA

Bilgi varlıklarının korunması ve ağ güvenliğinin sağlanması için; bilgi sınıflandırması, erişim kontrolü, ağ altyapısı güvenliği ve politika yönetimi gibi çeşitli bileşenleri içeren yaklaşımlar devreye alınmalıdır. Bu doğrultuda;

- **Bilgi Varlıklarının Tanımlanması ve Sınıflandırılması:** İlk olarak, şirket içinde bulunan tüm bilgi varlıkları tanımlanmakta ve sınıflandırılmalıdır. Bu, müşteri verileri, finansal bilgiler, ticari sırlar, personel dosyaları gibi çeşitli bilgi türlerini içerir. Bilgi varlıkları, gizlilik, bütünlük ve erişilebilirlik gibi kriterlere göre sınıflandırılmalıdır.
- **Erişim Kontrolü ve Yetkilendirme:** Belirlenen sınıflandırma düzeylerine göre, bilgi varlıklarına erişim yetkileri titizlikle yönetilmelidir. Roller ve yetkiler belirlenerek, her çalışanın sadece gereksinim duyduğu bilgilere erişimi sağlanmalıdır. Rol bazlı erişim kontrolü ve çok faktörlü kimlik doğrulama gibi güvenlik önlemlerini içermelidir.
- **Ağ Altyapısının Değerlendirilmesi ve Güvenliği:** Şirketimizin ağ altyapısı, belirlenen bilgi sınıflandırma düzeylerine uygun olarak yapılandırılmıştır. Ağ güvenliği önlemleri, güvenlik duvarları, ağ izleme sistemleri, saldırı tespit sistemleri ve güvenli ağ protokolleri gibi çeşitli teknolojileri içermektedir. Ağ cihazları ve yazılımları düzenli olarak güncellenmekte ve zayıf noktalar kapsamlı bir şekilde tespit edilmektedir.
- **Politika Yönetimi ve Uygulama:** Şirketimizde, bilgi güvenliği politikaları ve prosedürleri etkin bir şekilde uygulanmakta ve sürekli olarak gözden geçirilmektedir. Bu politikalar, bilgi varlıklarının korunması, ağ güvenliğinin sağlanması ve uygunluk standartlarının karşılanması için gerekli yönergeleri içermektedir. Ayrıca, çalışanlar düzenli eğitimlerle bilgilendirilmekte ve güvenlik bilinci artırılmaktadır.
- **Sürekli İyileştirme ve Denetim:** Yeni tehditler ve zayıf noktalar tespit edildiğinde, hızlı bir şekilde müdahale edilerek güvenlik önlemleri güncellenmektedir. Ayrıca, düzenli iç ve dış denetimler yapılarak uygunluk düzeyi değerlendirilmekte ve gerekli düzeltici önlemler alınmaktadır.

Ağ ekipmanı ve cihazlarının yönetiminden Bilgi İşlem Bölümü sorumludur. Ağ ekipmanı ve cihazlarının kurulumu, yapılandırılması, güncellenmesi, izlenmesi ve bakımıyla ilgili Bilgi İşlem personelleri tarafından dijital ortamda planlama çalışmaları gerçekleştirilerek yerinde uygulama (fiziksel montaj, ağ bağlantıları, yapılandırma ayarları ve güvenlik kontrolleri vb.) yapılır.

Ağ ekipmanlarının ve cihazlarının yapılandırma yönetimi, standart yapılandırma şablonları kullanılarak gerçekleştirilir. Bu şablonlar, güvenlik politikalarını ve performans gereksinimlerini karşılamak için önceden tanımlanmış ayarları içerir. Yazılım güncellemeleri, firmware güncellemeleri, donanım bakımı ve performans izleme gibi adımları içerir.

Ağ ekipmanları ve cihazları, sürekli olarak izlenir ve performans, güvenlik ve erişilebilirlik açısından değerlendirilir. Sorunlar tespit edildiğinde, hızlı bir şekilde müdahale edilir ve sorun giderme faaliyetleri gerçekleştirilir.

Ağ ekipmanları ve cihazlarının güvenliği; erişim kontrolleri, zayıf nokta taramaları, tehdit değerlendirmeleri ve sızma testleri gibi güvenlik önlemlerini içerir.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
30.01.2024	00/-	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

BGYS POLİTİKASI

Ağ ekipmanlarının (örneğin; yönlendiriciler ve anahtarlar) belgelerini, kullanım alanları, bağlantı şemaları, konfigürasyon, topoloji bilgileri vb. detaylı bilgilerini içeren bilgiler dokümante edilerek kayıt altına alınmakta ve gerekmesi durumunda revize edilmektedir.

Genel ağlar, üçüncü taraf ağlar veya kablosuz ağlar üzerinden geçen verilerin gizliliği ve bütünlüğünü korumak, bağlı sistemleri ve uygulamaları korumak amacıyla ağ trafiği şifreleme, güvenlik duvarı kullanımı, güvenlik protokolleri ve yetkilendirme mekanizmaları gibi teknik tedbirler uygulanmaktadır. Ayrıca, düzenli güvenlik taramaları ve izleme faaliyetleri gerçekleştirilerek ağ güvenliği durumu sürekli olarak izlenmekte ve değerlendirilmektedir. Ayrıca, ağ hizmetlerinin ve ağa bağlı bilgisayarların kullanılabilirliğini korumak için yedekleme ve kurtarma planlarının oluşturulması, ağ erişim politikalarının belirlenmesi ve uygulanması, güncel güvenlik yamalarının ve yazılım güncellemelerinin düzenli olarak yapılması gibi önlemler yer almaktadır.

Firma bünyesinde bilgi güvenliğini etkileyebilecek veya bununla ilgili eylemlerin kaydedilmesini ve tespit edilmesini sağlamak amacıyla uygun şekilde günlüğe kaydetme (log tutulması) ve izleme süreçleri uygulanmaktadır. Log tutma süreci, bilgi sistemlerinde meydana gelen olayların ayrıntılı bir şekilde kaydedilmesini ve saklanmasını sağlar. Şirketimizde, çeşitli sistemlerde (sunucular, ağ cihazları, güvenlik cihazları, uygulama sunucuları vb.) loglama yapılmaktadır. Bu loglar, genellikle olayın tarih ve saati, kullanıcı kimliği, olayın türü, işlem detayları ve diğer ilgili bilgileri içerir. Loglar, belirli bir standart veya format kullanılarak oluşturulur ve belirli bir süre boyunca saklanır.

Bu log tutma ve izleme süreçleri, şirketimizde bir dizi alanda uygulanmaktadır:

- Kullanıcı oturumları ve yetkilendirme denemeleri
- Ağ trafiği ve güvenlik duvarı olayları
- Sunucu ve sistem etkinlikleri
- Güvenlik olayları ve saldırılar

Bu süreçler, bilgi güvenliği ihlallerini tespit etmek, hızlı bir yanıt sağlamak ve gelecekteki tehditleri önlemek için önemlidir. Ayrıca, uygun izleme ve log tutma uygulamaları, mevzuat gereksinimlerine uyumu sağlamak ve denetimlerde kullanılmak üzere gereklidir. Şirketimiz, bilgi güvenliği izleme ve log tutma süreçlerini sürekli olarak gözden geçirerek ve iyileştirme çalışmaları yapmaktadır. Bu sayede, bilgi sistemlerinin güvenliği ve bütünlüğü sürekli olarak koruması ve geliştirilmesi sağlanır.

İzleme faaliyetleri kapsamında, Güvenlik Bilgi ve Olay Yönetimi (SIEM) sistemleri kullanılmaktadır. SIEM sistemleri, ağ ve sistem güvenliği ile ilgili olayların izlenmesi, analiz edilmesi ve raporlanmasını sağlayan entegre bir çözümdür. SIEM ürünü, ağdaki güvenlik olaylarını ve aktiviteleri izlemek, tespit etmek ve raporlamak için kullanılmaktadır. Bu sistem, farklı kaynaklardan gelen günlük verilerini toplar, bir araya getirir ve analiz eder. Ardından, potansiyel tehditler ve anormallikler belirlenerek ilgili personel tarafından incelenir ve gerekli önlemler alınır.

SIEM sistemi, güvenlik olaylarını gerçek zamanlı olarak izler ve analiz ederken aynı zamanda tespit edilen olayları bir veri tabanında kaydeder. Bu kayıtlar, şüpheli aktivitelerin izlenmesi ve geçmiş olayların analizi için kullanılır. Ayrıca, SIEM sistemi, güvenlik politikalarının uygulanmasını değerlendirmek ve güvenlik açıklarını tespit etmek için kullanılabilir.

Şirketimizdeki SIEM sistemi, bilgi işlem personeli tarafından düzenli olarak izlenir ve yönetilir. Bu personel, günlük olarak SIEM araçlarını kullanarak sistemdeki güvenlik olaylarını ve aktiviteleri inceler. Tespit edilen herhangi bir anormallik veya güvenlik tehdidi durumunda, ilgili önlemler hızla alınarak güvenlik açığı kapatılır ve sistem korunur. Bu sayede, şirketimizdeki bilgi güvenliği etkin bir şekilde sağlanmış olur.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
30.01.2024	00/-	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

BGYS POLİTİKASI

Bilgi işlem birimi, ağ altyapısının planlanması, kurulması, yapılandırılması ve yönetilmesinden sorumludur. Bu kapsamda, ağ bileşenlerinin (örneğin, yönlendiriciler, anahtarlar, sunucular) kurulumu ve yapılandırılması, ağ erişim politikalarının belirlenmesi ve uygulanması gibi faaliyetler yürütülür.

Ağ yönetimi faaliyetleri, farklı departmanlar arasında yakın işbirliği ve iletişim gerektirir. Örneğin, ağ altyapısının güvenliği, bilgi güvenliği ekibiyle birlikte planlanır ve uygulanır. Ayrıca, ağ performansının izlenmesi ve iyileştirilmesi, operasyonel departmanlarla işbirliği içinde gerçekleştirilir.

Bilgi işlem birimi, ağ yönetimi faaliyetlerini koordine ederken aynı zamanda kuruluşun iş ihtiyaçlarını da dikkate alır. Bu sayede, ağ altyapısı hem kuruluşun ihtiyaçlarını karşılar hem de bilgi işleme politikaları ve standartlarına uygun olarak yönetilir. Bu yaklaşım, hizmet kalitesini artırırken aynı zamanda güvenlik ve uyumluluk gereksinimlerini de karşılar.

Ağ üzerindeki sistemlere erişim sırasında kimlik doğrulama süreci titizlikle uygulanır. Bu süreç, kullanıcıların kimliklerinin doğrulanması ve yetkilendirilmiş erişim haklarının belirlenmesi için kullanılır. Kimlik doğrulama süreci genellikle kullanıcı adı ve parola gibi bilgilerin girilmesiyle başlar. Şirketimizde, bu bilgilerin yanı sıra ek güvenlik katmanları da kullanılabilir. Örneğin, çift faktörlü kimlik doğrulama gibi yöntemlerle kullanıcıların kimlikleri daha güvenli bir şekilde doğrulanabilir. Kimlik doğrulama süreci, ağ üzerindeki sistemlerin güvenliğini sağlamak için düzenli olarak gözden geçirilir ve güncellenir.

Sistemlerin ağa bağlantısının kısıtlanması ve filtrelenmesi, ağ güvenliğini sağlamak için kritik bir öneme sahiptir. Şirketimizde, bu önlemler alınarak ağ üzerindeki sistemlerin güvenliği artırılmaktadır. Bu kapsamda, şirketimizde güvenlik duvarları gibi ağ güvenlik cihazları kullanılarak sistemlerin ağa bağlantısı kısıtlanır ve filtrelenir. Güvenlik duvarları, ağ trafiğini denetleyerek gelen ve giden verilerin güvenliğini sağlar. Bu cihazlar, belirlenmiş olan güvenlik politikalarına göre trafiği izler ve istenmeyen veya tehlikeli trafiği engeller. Sistemlerin ağa bağlantısının kısıtlanması ve filtrelenmesiyle şirketimizde şu hedeflerin gerçekleştirilmesi amaçlanmaktadır;

- Güvenlik Duvarlarının Kullanılması
- Erişim Kontrolü
- Tehditlerin Engellenmesi
- Veri Gizliliği ve Bütünlüğü

Ekipman ve cihazların ağa bağlantısının tespit edilmesi, kısıtlanması ve doğrulanması faaliyetleri şu şekilde gerçekleştirilir;

- **Tespit Etme:** Ağ envanteri yönetimi yazılımları veya ağ izleme araçları kullanılarak gerçekleştirilir. Bu araçlar, ağdaki her bir cihazın IP adresini, MAC adresini, bağlantı noktalarını ve diğer ilgili bilgileri belirler. Ayrıca, bu süreçte ağdaki cihazların türleri, markaları ve modelleri de belirlenir.
- **Kısıtlama ve Doğrulama:** Tespit edilen cihazların ağa bağlantısı, şirketimizin belirlediği güvenlik politikalarına uygun olup olmadığı incelenir. Bu politikalar, belirli cihazların belirli ağ kaynaklarına erişimini kısıtlayabilir veya izin verebilir. Örneğin, bir depolama sunucusuna erişim izni sadece belirli bir departmanın belirli bir cihazına verilebilir. Bu doğrulama ve kısıtlama işlemleri, ağ güvenlik duvarları, ağ anahtarları ve benzeri ağ yönetim cihazları aracılığıyla gerçekleştirilir.
- **Ekipman ve Cihaz Doğrulaması:** Ağa bağlanan her cihazın kimliği ve güvenilirliği doğrulanır. Bu doğrulama süreci, cihazların benzersiz kimlik bilgileriyle gerçekleştirilir. Bu bilgiler genellikle cihazların MAC adresi, seri numarası veya diğer benzersiz tanımlayıcıları olabilir. Ayrıca, cihazların yetkilendirilmiş bir kullanıcı veya sistem tarafından kullanıldığından emin olunur. Örneğin, bir bilgisayarın ağa bağlantısı, çalışanın kimlik doğrulamasıyla ilişkilendirilir ve sadece yetkilendirilmiş kullanıcılar tarafından kullanılabilir.

Bu adımların tamamlanmasıyla, şirketimizin ağ altyapısındaki cihazların güvenliği sağlanır ve yetkisiz erişimler önlenir. Herhangi bir güvenlik ihlali veya risk tespit edildiğinde, gerekli önlemler hızla alınır ve güvenlik duvarları gibi cihazların

konfigürasyonları düzenli olarak gözden geçirilir ve güncellenir. Bu süreçlerin etkin bir şekilde yürütülmesi, şirketimizin ağ güvenliğini korumak için kritik bir öneme sahiptir.

Ağ cihazlarının güçlendirilmesi, şirketimizin ağ güvenliğini artırmak ve saldırılara karşı korunmak için kritik öneme sahip bir süreçtir. Bu süreç, ağ cihazlarının (örneğin, yönlendiriciler, anahtarlar, güvenlik duvarları vb.) güvenlik düzeyini artırmak için özel bir dizi teknik ve prosedürü içerir. Bu kapsamda; güvenlik güncellemeleri ve yama uygulamaları, güçlü kimlik doğrulama ve yetkilendirme, erişim kontrol listeleri (ACL) kullanımı, zararlı yazılım ve saldırı tespit sistemleri (IDS/IPS), güvenlik duvarları ve sanal özel ağlar (VPN) çalışmalar yürütülmektedir. Bu çalışmaların düzenli olarak uygulanması, şirketimizin ağ cihazlarının güçlendirilmesini ve ağ güvenliğinin sağlanmasını sağlamaktadır. Ayrıca, güçlendirme süreci düzenli olarak gözden geçirilmesi ve güncellenmesiyle ağ güvenliği sürekli olarak optimize edilerek ve güçlendirilmektedir.

Ağ yönetim kanallarının diğer ağ trafiğinden ayrılması, ağ yöneticilerinin ağ cihazlarına erişmek için kullandığı özel iletişim kanallarının diğer ağ trafiğinden ayrılması amacıyla gerçekleştirilmektedir. Bu uygulama ağ yönetim trafiğinin diğer ağ trafiğinden izole edilmesini ve önceliklendirilmesini sağlayarak ağ yönetimi için ayrılan kaynakların maksimum verimlilikle kullanılmasına imkan tanımaktadır.

Firmamızda ağ yönetim kanallarının diğer ağ trafiğinden ayrılması için izlenen yöntemler şunlardır:

- **Ağ Yönetim VLAN'ları (Virtual Local Area Network):** Ağ yönetim trafiği için özel VLAN'lar oluşturulur. Bu VLAN'lar, ağ yöneticilerinin erişim sağladığı cihazlar arasında iletişimi sağlar ve diğer kullanıcı trafiğinden ayrı bir ağ segmenti oluşturur.
- **Ağ Yönetim Protokolleri ve Portları:** Ağ yöneticileri genellikle SNMP (Simple Network Management Protocol), SSH (Secure Shell), veya HTTPS (Hypertext Transfer Protocol Secure) gibi güvenli protokoller aracılığıyla ağ cihazlarına erişir. Bu protokollerin kullanımı, ağ yönetim trafiğini diğer ağ trafiğinden ayırır ve güvenli bir iletişim sağlamaktadır.
- **Trafiği Yönlendirme ve QoS (Quality of Service):** Ağ yönetim trafiği için öncelikli bir hizmet sınıfı belirlenir ve bu trafiğin diğer kullanıcı trafiğinden öncelikli olarak yönlendirilmesi sağlanır. Bu, ağ yönetim trafiğinin diğer trafiğe göre önceliğini korur ve kesintisiz bir yönetim deneyimi sağlar.
- **Güvenlik Duvarları ve Erişim Kontrol Listeleri (ACL):** Ağ yönetim kanallarına erişim, güvenlik duvarları ve erişim kontrol listeleri (ACL) gibi güvenlik önlemleriyle korunur. Bu önlemler, yetkisiz erişimleri engeller ve ağ yönetim trafiğini güvenli bir şekilde izole eder.

Ağ saldırı altında kritik alt ağların geçici olarak yalıtılması, şirketimizin ağ güvenliği politikasının önemli bir parçasını oluşturmaktadır. Ağ saldırısı algılandığında veya şüphelenildiğinde, kritik alt ağlar, saldırıdan etkilenen diğer ağ segmentlerinden izole edilir. Bu izolasyon süreci, öncelikle köprü işlevi yapan cihazlar aracılığıyla gerçekleştirilebilir.

Köprü işlevi yapan cihazlar, ağ trafiğini farklı ağ segmentleri arasında ileten ve yönlendiren ağ cihazlarıdır. Saldırı algılandığında, bu cihazlar, kritik alt ağların ağdan geçici olarak izole edilmesini sağlayarak, saldırının yayılmasını engellemek için kullanılır. Bu izolasyon süreci, kritik alt ağların normal ağ trafiğinden geçici olarak ayrılmasını sağlar ve saldırıya hedef olan segmentlerin zarar görmesini önlemektedir.

Şirketimizde, bu tür ağ saldırılarını tespit etmek ve müdahale etmek için gelişmiş güvenlik sistemleri ve izleme araçları kullanılmaktadır. Ayrıca, kritik alt ağların izolasyonu ve saldırıya karşı korunması konusunda belirlenmiş acil durum prosedürleri ve politikaları bulunmaktadır. Bu sayede, ağ saldırılarına karşı etkili bir şekilde mücadele edilir ve şirketin ağ güvenliği sağlanmış olur.

Savunmasız ağ protokollerinin devre dışı bırakılması için şu adımlar izlenir:

- **Protokollerin İncelenmesi:** Öncelikle, mevcut ağ yapısındaki kullanılan protokoller detaylı bir şekilde incelenir ve değerlendirilir. Hangi protokollerin savunmasız olduğu ve potansiyel güvenlik riskleri taşıdığı belirlenir.
- **Gereksiz Protokollerin Devre Dışı Bırakılması:** İnceleme sonucunda, savunmasız veya gereksiz olduğu belirlenen ağ protokolleri belirlenir ve bu protokollerin devre dışı bırakılması kararlaştırılır. Bu adım, ağdaki gereksiz protokollerin kullanılmamasını sağlar ve saldırılara karşı potansiyel riskleri azaltır.
- **Güvenli Alternatiflerin Kullanımı:** Savunmasız protokollerin devre dışı bırakılmasıyla birlikte, daha güvenli ve güncel protokollerin kullanımı teşvik edilir. Bu, ağdaki güvenlik seviyesini artırır ve potansiyel saldırı vektörlerini azaltır.
- **Sürekli İzleme ve Güncelleme:** Ağdaki protokollerin güvenlik durumu düzenli olarak izlenir ve güncellenir. Yeni güvenlik açıkları veya tehditler ortaya çıktığında, gerekli önlemler alınarak ağın korunması sağlanır.