BGYS POLİTİKASI

Politika Numarası	PLTK-24
Politika Tanımı	Kullanıcı Uç Nokta Cihazları Güvenlik Politikası
Amaç ve İlkeler	**Bu politika,** kullanıcı uç nokta cihazlarının güvenliğini sağlamak ve bu cihazlar üzerinde işlenen bilgilerin korunmasını temin etmektir. Bu politika, fiziksel ve yazılım düzeyindeki güvenlik önlemlerini belirleyerek, kullanıcı uç nokta cihazlarının güvenliğini artırmayı ve bilgi güvenliği risklerini en aza indirmeyi hedeflemektedir.
Sorumluluklar	**Bilgi İşlem Personeli:** Politika dışı davranılmasının engellenmesi amacıyla sistem kurulması ve kurulan sistemin denetlenmesinden sorumludur. **Tüm çalışanlar:** Belirlenen politika ve prosedürlere uymakla yükümlüdür.
Sapma ve Özel Durumlar	Sapmalar veya özel durumlarla karşılaşıldığında, ilgili departman veya yöneticilerle iletişime geçilmelidir. Bu durumlar, politikanın etkinliğini artırmak için incelenir ve gerekli düzeltici önlemler alınarak, uygun cezai yaptırımlar gerçekleştirilir.

UYGULAMA

Kullanıcı uç nokta cihazları, genellikle şirket çalışanları tarafından kullanılan dizüstü bilgisayarlar, masaüstü bilgisayarlar, tabletler ve akıllı telefonlar gibi cihazlardır. Bu cihazlar, çalışanların günlük işlerini yapmaları için kullandıkları araçlardır. Bu cihazlar üzerinde işlenen bilgilerin türü ve bu bilgilerin önemi, şirketin bilgi güvenliği açısından büyük önem taşımaktadır.

Kullanıcı uç nokta cihazlarının kaydı FR.383 Varlık Envanteri Formu içerisinde tutulmalıdır.

Uç nokta cihazlarının fiziksel olarak korunması için kilitli odalar, güvenlik kameraları, alarm sistemleri, fiziksel etiketleme gibi önlemler alınmalıdır.

Kullanıcı uç nokta cihazları, işlenen bilgilerin hassaslık düzeyine göre sınıflandırılmalıdır. Bu cihazlar üzerinde sınıflandırma seviyelerine uygun olarak işlenmesi gereken bilgiler belirlenmelidir.

Her kullanıcı uç nokta cihazı, kayıt altına alınmalıdır. Bu kayıtlar, cihazın özellikleri, konumu, sahibi ve kullanım amacını içermelidir.

Kullanıcı uç nokta cihazları, fiziksel olarak güvenli bir ortamda bulundurulmalıdır. Yetkisiz erişime karşı korunmalı ve gerekirse ek fiziksel koruma önlemleri alınmalıdır.

Yalnızca gereksinim duyulan yazılım ve uygulamalar kullanıcı uç nokta cihazlarına yüklenmelidir. Kurulumlar, belirlenen güvenlik standartlarına uygun olarak yapılmalıdır.

Kullanıcı uç nokta cihazlarındaki yazılımlar ve işletim sistemleri düzenli olarak güncellenmelidir. Bu güncellemeler, otomatik veya manuel olarak yapılabilir.

Ağ bağlantıları, belirlenen güvenlik protokollerine uygun olarak yapılandırılmalıdır. Bağlantılar şifrelenip kişisel güvenlik duvarları kullanılmalıdır.

Bilgilere erişim, yetkilendirilmiş personel tarafından sağlanmalıdır. Hassas veya kritik bilgilere erişim, ihtiyaç halinde ve yetkilendirilmiş personel tarafından yapılmalıdır.

Depolama cihazları şifrelenmelidir. Bu, cihazın kaybolması veya çalınması durumunda verilerin güvende olmasını sağlayacaktır.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
05.02.2024	-	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

BGYS POLİTİKASI

Kullanıcı uç nokta cihazları, kötü amaçlı yazılımlara karşı korunmalıdır. Antivirüs ve antimalware yazılımları düzenli olarak güncellenmeli ve kullanıcılar bu konuda eğitilmelidir.

Çalışanlar, kullanıcı uç nokta cihazlarının çalınması veya kaybolması durumunda derhal İnsan Kaynakları veya Bilgi İşlem Departmanı ile iletişime geçmelidir. Bu bildirim, en kısa sürede ve mümkün olan en yüksek öncelikle yapılmalıdır. Kaybolan veya çalınan cihazlar içindeki bilgilerin korunması için uzaktan etkisiz hale getirilmelidir. Mobil cihazların kayıp veya çalıntı durumunda, cihazın son bilinen konumu tespit edilmelidir.

İş verilerinin güvenliği, veri kaybını önlemek ve hassas bilgilerin kötü niyetli kişilerin eline geçmesini engellemek amacıyla eğer mümkünse, cihazda bulunan iş verileri uzaktan silinmelidir. Olay, ayrıntılı bir şekilde incelenmeli ve kayıp veya çalıntı cihazın neden olduğu olası güvenlik açıkları belirlenmelidir.

Kullanıcı uç nokta cihazlarında yazılım kurulumunu kısıtlamak ve yönetmek amacıyla;

- **Uzaktan Yönetim Araçları:** Sistem yöneticileri tarafından kullanıcı uç nokta cihazlarına erişebilmek ve yazılım kurulumlarını yönetmek için uzaktan yönetim araçları kullanmalıdır. Bu sayede, gereksinim duyulan güncellemeler kolayca ve güvenli bir şekilde uygulanabilmektedir.
- **Yazılım Kısıtlamaları:** Kullanıcı uç nokta cihazlarına yüklenen yazılımları sınırlamak için belirli politikalar belirlenmelidir. Yalnızca belirlenen onaylı yazılımların veya uygulamaların yüklenmesine izin verilmeli, potansiyel olarak zararlı veya güvenlik riski taşıyan yazılımların yüklenmesi engellenmelidir.
- **Otomatik Güncelleme Politikası:** Kullanıcı uç nokta cihazlarında çalışan yazılımların ve uygulamaların otomatik güncelleme özelliği etkinleştirilmelidir. Bu sayede, güvenlik açıkları zamanında kapatılmakta ve cihazların güvenliği güncel tutulmaktadır.
- **Yazılım Sürüm Kontrolleri:** Kullanıcı uç nokta cihazlarında çalışan yazılımların sürüm kontrolü düzenli olarak gerçekleştirilmelidir. Güncel olmayan veya desteklenmeyen yazılım sürümleri tespit edilerek, güncellenmesi veya kaldırılması gereken yazılımlar belirlenmektedir.

Kullanıcı uç nokta cihazlarında otomatik güncelleme özelliği devre dışı bırakılmalı ve güncellemeler manuel olarak yönetilmelidir.

Kullanıcı uç nokta cihazlarının bilgi hizmetlerine, genel ağlara veya tesis dışındaki herhangi bir ağa bağlantısı için uyulması gereken kurallar aşağıdaki gibidir;

- **Kişisel Güvenlik Duvarı Kullanımı:** Kullanıcı uç nokta cihazlarına, bilgi hizmetlerine, genel ağlara veya tesis dışındaki herhangi bir ağa bağlantı için kişisel güvenlik duvarı kullanımı zorunlu tutulmalıdır. Bu güvenlik duvarı, cihazın iç ve dış tehditlere karşı korunmasını sağlar ve yetkisiz erişimleri engellemektedir.
- **Ağ Erişim Kontrolleri:** Kullanıcı uç nokta cihazlarının bilgi hizmetlerine veya genel ağlara erişimini kısıtlamak için ağ erişim kontrolleri uygulanmalıdır. Bu kontroller, belirlenen güvenlik politikalarına uygun olmayan erişimleri engellemekte ve güvenliğin korunmasını sağlamaktadır.
- **VPN Kullanımı:** Tesis dışındaki ağlara erişim için sanal özel ağ (VPN) kullanımı teşvik edilmelidir. VPN, kullanıcı uç nokta cihazlarının internet üzerinden güvenli bir şekilde bağlanmasını ve verilerin şifrelenerek korunmasını sağlamaktadır.

Erişim kontrolleri konusunda gerçekleştirilecek çalışmalar şunları içermelidir;

- **Kimlik Doğrulama ve Yetkilendirme:** Kullanıcıların kimliklerini doğrulamak ve uygun yetkilere sahip olmalarını sağlamak için kimlik doğrulama ve yetkilendirme politikaları belirlenmelidir. Bu politikalar, kullanıcıların güvenli parola seçmelerini, iki faktörlü kimlik doğrulama kullanmalarını ve gerektiğinde yetkilendirme seviyelerini gözden geçirmelerini içermelidir.

- **İzin Kontrolleri ve Rol Tabanlı Erişim:** Kullanıcıların erişim hak ve izinleri rol tabanlı erişim kontrolü (Role-Based Access Control - RBAC) yöntemiyle yönetilmelidir. Bu yöntem, kullanıcıların görev ve sorumluluklarına göre belirlenen roller aracılığıyla erişim izinlerinin atanmasını ve yönetilmesini sağlayacaktır.
- **Günlük Tutma ve İzleme:** Erişim kontrollerini izlemek ve denetlemek için günlük tutma ve izleme sistemleri kullanılmalıdır. Bu sistemler, kullanıcıların erişim faaliyetlerini, izin değişikliklerini ve diğer ilgili olayları kaydederek, yetkilendirilmemiş erişim girişimlerini tespit etmeye ve önlem almaya yardımcı olacaktır.

Verilerin yetkisiz erişimden korunmasını amacıyla depolandığı cihazların (örneğin, sabit diskler, USB sürücüler, harici diskler) şifrelenmesi işlemi yapılmalıdır. Bu kapsamda yapılacak çalışmalar;

- **Tam Disk Şifrelemesi:** Tüm bilgisayar ve mobil cihazlarda tam disk şifrelemesi uygulanmalıdır. Çalışanların cihazları kaybolması veya çalınması durumunda dahi verilerimiz güvende olmaktadır.
- **Veri Depolama Standartlarının Belirlenmesi:** Depolama cihazlarında kullanılan şifreleme standartları belirlenmeli ve tüm cihazlarda bu standartlara uygun şifreleme yöntemleri kullanılmalıdır.
- **Yazılım Güncelleme:** Yazılım tabanlı şifreleme çözümlerimiz sürekli olarak güncellenmekte ve en son güvenlik yamaları ile donatılmaktadır. Bu sayede, potansiyel güvenlik açıkları kapatılarak verilerimizin güvenliği sağlanmaktadır.

Kötü amaçlı yazılımların bilgisayar sistemlerine zarar vermesini önlemek ve güvenliği sağlamak için end point security ürünleri kullanılmalıdır. Bu ürünler, kullanıcıların bilgisayarlarında veya diğer cihazlarda kötü amaçlı yazılımların tespit edilmesi ve engellenmesi için güçlü bir koruma sağlayacaktır.

End point security ürünleri, bilgisayarların işletim sistemleri ve uygulamaları üzerinde sürekli olarak izleme yapar ve potansiyel tehditleri algılar. Virüsler, truva atları, kötü amaçlı yazılımlar ve diğer zararlı yazılımlar gibi tehditler tespit edildiğinde, bu ürünler otomatik olarak önlem alır ve saldırıları engeller.

Bu end point security çözümleri ayrıca, kötü amaçlı yazılımların bilgisayar sistemlerine bulaşmasını önlemek için proaktif olarak davranır. Güvenlik duvarı, antivirüs yazılımı, kötü amaçlı yazılım taraması ve diğer koruma özellikleri, bilgisayarlarımızı ve ağımızı güvende tutmak için bir araya getirilir.

End point security ürünlerinin düzenli olarak güncellenmesi sağlanmalı ve bu ürünlerin en son tehditlere karşı güncel olduğundan emin olunmalıdır. Ayrıca, çalışanlara bu ürünlerin nasıl kullanılacağı konusunda eğitimler verilmeli ve güvenlik politikalarına uygun şekilde hareket etmeleri teşvik edilmelidir.

Uzaktan devre dışı bırakma, silme veya kilitleme gibi önemli güvenlik önlemlerini sağlamak için Bitdefender ürünleri kullanılmalıdır.

Yedekleme işlemleri aşağıdaki gibi gerçekleştirilmelidir;

- **Düzenli Yedekleme:** Tüm kritik veriler düzenli (günlük, haftalık ve aylık vb.) otomatik olarak yedeklenmelidir.
- **Farklı Depolama Ortamları:** Yedek veriler farklı depolama ortamlarına kaydedilmelidir. Böylece, bir depolama cihazı veya ortamı başarısız olduğunda bile verilerin kaybedilme riski en aza indirilmelidir.
- **Veri Kurtarma Denemeleri:** Düzenli olarak yedeklenen verilerin geri yüklenmesi ve doğrulanması için periyodik olarak veri kurtarma denemeleri yapılmalıdır.
- **Kapsamlı Yedekleme:** Hangi verilerin yedekleneceği, ne sıklıkta yedekleme yapılacağı, yedeklemelerin nerede saklanacağı ve nasıl korunacağı belirlenmelidir.
- **Güvenlik ve Şifreleme:** Yedek verileri, güvenli depolama ortamlarında şifrelenip yetkisiz erişime karşı korunmalıdır.
- **Yedekleme Süreçlerinin İzlenmesi:** Yedekleme süreçleri düzenli olarak izlenip denetlenmelidir. Herhangi bir hata veya başarısızlık durumunda hızlı bir şekilde müdahale edilmeli ve sorun giderilmelidir.

Web servisleri ve web uygulamalarının kullanımı konusunda;

- **Yetkilendirme ve Yetkilendirme Kontrolleri:** Web servislerine ve uygulamalarına erişim, kullanıcıların yetkilendirilmesi ve yetkilendirme kontrolleri ile sınırlandırılmalıdır. Sadece belirli kullanıcı rolleri veya departmanlar, belirli web servislerine veya uygulamalara erişebilmelidir.
- **Güvenlik Duvarı ve Ağ Filtreleme:** Şirket ağına giriş ve çıkış trafiği, potansiyel tehditlerin önlenmesi ve kötü amaçlı yazılımların tespit edilmesi için güvenlik duvarları ve ağ filtreleme cihazları tarafından izlenip denetlenmelidir.
- **Güvenlik Güncelleştirmeleri:** Web servisleri ve uygulamaları için kullanılan yazılım ve platformların güvenlik güncelleştirmeleri düzenli olarak uygulanmalıdır.
- **Veri Güvenliği:** Web servisleri ve uygulamaları üzerinde taşınan ve işlenen veriler, gerekli güvenlik önlemleri alınarak korunmalıdır. Bu verilerin güvenliği için şifreleme, kimlik doğrulama ve yetkilendirme yöntemleri kullanılmalıdır.

Son kullanıcı davranışı analitiği çözümlerini kullanarak bilgi güvenliğini artırılmalıdır. Bu çözümler, kullanıcıların bilgisayarlarını ve diğer cihazlarını kullanırken gösterdikleri davranışları izler ve anormal aktiviteleri tespit ederek potansiyel güvenlik tehditlerini belirleyecektir. Bu çalışmalar şu avantajları sağlayacaktır;

- **Anormal Davranış Tespiti:** Kullanıcıların normal iş rutinlerinden sapma durumlarında uyarılar verilir. Örneğin, normalde erişilmeyen bir sistem veya uygulamaya erişim denemesi gibi anormal aktiviteler tespit edilebilir.
- **Veri İhlali Tespiti:** Hassas verilere erişim veya bu verilerin izinsiz aktarımı gibi potansiyel veri ihlalleri tespit edilir. Bu sayede, veri ihlalleri hızlı bir şekilde tespit edilerek müdahale edilebilir.
- **Kimlik Hırsızlığı Tespiti:** Kullanıcı kimlikleri üzerinde yapılan anormal aktiviteler tespit edilir. Örneğin, kullanıcı hesaplarının izinsiz olarak kullanılması veya paylaşılması gibi durumlar belirlenebilir.
- **Gelişmiş Teşhis ve Analiz:** Son kullanıcı davranışı analitiği çözümleri, detaylı teşhis ve analiz imkanı sağlar. Bu sayede, güvenlik olaylarının kökeni belirlenebilir ve benzer olayların önlenmesi için önlemler alınabilir.
- **Otomatik Uyarılar ve Müdahale:** Anormal aktiviteler tespit edildiğinde otomatik uyarılar oluşturulur ve gerektiğinde otomatik müdahaleler yapılır. Bu sayede, güvenlik ekibi hızlı bir şekilde potansiyel tehditlere karşı harekete geçebilir.

Çıkarılabilir aygıtların kullanımı ve fiziksel bağlantı noktalarının kontrol altında tutulması için;

- **Çıkarılabilir Aygıtların Kullanımının Sınırlanması**: Çalışanların, şirket bilgisayarlarına çıkarılabilir aygıtlar bağlaması veya kullanması sınırlandırılmalıdır. Bu aygıtların kullanımı, güvenlik risklerini en aza indirmek amacıyla gereksinimlere göre belirlenmiş ve yetkilendirilmiş personel tarafından yapılmalıdır.
- **Yetkilendirilmiş Aygıtların Tanımlanması:** Şirket politikalarına uygun olan ve güvenlik kontrollerinden geçmiş çıkarılabilir aygıtlar, önceden belirlenmiş bir liste dahilinde tanımlanmalıdır. Bu sayede, yalnızca güvenilir ve gereksinimlere uygun aygıtların kullanımına izin verilmelidir.
- **Fiziksel Bağlantı Noktalarının Denetlenmesi:** USB ve diğer çıkarılabilir aygıt bağlantı noktaları, gereksinim dâhilinde denetlenmeli ve güvenlik kontrolleriyle korunmalıdır. Yetkilendirilmemiş aygıtların bu noktalara bağlanması engellenmeli veya izlenmelidir.
- **Gereksinimlere Uygun Şifreleme:** Çıkarılabilir aygıtların kullanımı gerektiğinde, veri şifrelemesi zorunlu tutulmalıdır. Bu, aygıtın kaybolması veya çalınması durumunda verilerin korunmasını sağlayacaktır.
- **İzleme ve Denetleme:** Çıkarılabilir aygıt kullanımı ve bağlantı noktaları düzenli olarak izlenip denetlenmelidir.

Firma bünyesinde kullanılan merkezi sunucu yapısıyla kritik öneme sahip tüm verilerin sunucularda tutulması sağlanmalıdır. Her kullanıcı kendisine açılan hesap bilgileri ile bu sunuculara erişim sağlayıp işlemlerini yapabilmelidir.

Kullanıcı Sorumluluğu

Tüm çalışanlar, kullanıcı uç nokta cihazlarını korumaya yönelik güvenlik gereklilikleri ve prosedürleri titizlikle uygulamalıdır. Çalışanlar bu güvenlik önlemlerini etkili bir şekilde yerine getirmek için aşağıdaki tavsiyelere uymalıdır;

- **Aktif Oturumları Kapatmak ve Hizmetleri Sonlandırmak:** Kullanıcılar, işlerini tamamladıklarında veya cihazlarını kullanmayacakları durumlarda aktif oturumları kapatmalı ve gereksiz hizmetleri sonlandırmalıdır.
- **Fiziksel ve Mantıksal Kontrollerle Koruma**: Uç nokta cihazları kullanılmadıkları zamanlarda fiziksel kontrol önlemleri (tuş kilidi, özel kilitler) ve mantıksal kontrol yöntemleri (şifre erişimi) ile yetkisiz kullanıma karşı korunmalıdır. Özellikle önemli, hassas veya kritik iş bilgilerini içeren cihazlar gözetimsiz bırakılmamalı ve güvenlik en üst düzeyde sağlanmalıdır.
- **Özel Dikkatle Kullanım:** Cihazlar, halka açık yerlerde, açık ofislerde, toplantı yerlerinde ve diğer korunmasız alanlarda özel dikkatle kullanılmalıdır. Örneğin, gizli bilgilerin izinsiz erişimini engellemek amacıyla gizlilik ekranı filtreleri kullanılmakta ve insanların gizli bilgileri görmeleri önlenmektedir.
- **Fiziksel Koruma Önlemleri**: Kullanıcılar, cihazlarını hırsızlığa karşı fiziksel olarak korumak adına gerekli önlemleri almalıdır. Arabalar ve diğer ulaşım şekillerinde, otel odalarında, konferans merkezlerinde ve toplantı yerlerinde cihazlar güvenli bir şekilde saklanmalı ve potansiyel risklere karşı tedbirler alınmalıdır.

Kişisel cihazların kullanımı

İş verilerinin güvenliğini sağlamak ve bilgi güvenliği standartlarını korumak amacıyla iş ortamında kişisel cihazların (telefon, tablet vb.) kullanımına izin verilmemelidir. Çalışanlar iş gereksinimleri için sadece firma tarafından sağlanan cihazları kullanmalıdır.