İÇİNDEKİLER

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

1. Amaç

Bu politikanın amacı kablosuz cihazların firmanın bilişim güvenliğini riske etmeden bilgisayar ağımıza entegre edilmesi için söz konusu cihazların sahip olması gereken minimum standartları tanımlamaktır.

Kablosuz iletişim ağı bu ESOGÜ BİDB genel ağ altyapısının bir parçası olduğunda, kablosuz iletişim ağlarının tasarımı, kurulumu ve yönetimi ağın güvenliği açısından önem arz etmektedir

2. Kapsam

Bu politika, ESOGÜ BİDB ağına bağlanan tüm kablosuz bağlantılar için geçerlidir.

ESOGÜ bünyesinde kullanılabilecek kablosuz veri transferi sağlayabilen herhangi bir cihaz bu politikanın kapsamındadır.

3. Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi

BİDB: Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. Sorumlular

Bu prosedürün oluşturulmasından Bilgi Güvenliği Birimi sorumludur. Bu süreçte BGYS Yöneticisi ile beraber çalışmak IT Yöneticisi sorumluluğundadır.
Politikanın uygulanmasından IT Yöneticisi ve teknik ekibi sorumludur.

5. Kurallar

ESOGÜ BİDB sorumluluğundaki tüm Kablosuz iletişim ağları IT Yöneticisi ve ekibi tarafından izlenir ve muhafaza edilir. ESOGÜ BİDB ağ altyapısına bağlı/bağlanan herhangi bir Erişim Noktası (Access Point) veya kablosuz cihaz, ESOGÜ BİDB sorumluluğu altında kabul edilir.
Aşağıdaki kurallar bu politikanın uygulama esasları olarak tanımlanmıştır.

- Personelin ESOGÜ ağında kullandığı tüm Erişim Noktalarının ve kablosuz cihazlarının, kablosuz ağın ilgili tüm yasal düzenlemelerine, standartlarına ve IT Yöneticisi tarafından tanımlanmış kurallara uygun olması gerekir.
- IT Yöneticisi tarafından onaylanan kablosuz ağ erişim cihazları kullanılmalıdır.
- Standart olmayan Erişim Noktalarının veya kablosuz cihazların kurulumu yasaktır.
- Kablosuz erişim cihazlarında, ESOGÜ BİDB'nin belirlemiş olduğu güvenlik ayarları kullanılmalıdır.
- Erişim cihazlarının tamamı ESOGÜ BİDB'nin fiziksel olarak korunmuş alanı içinde konumlandırılmalıdır.
- ESOGÜ BİDB, mevcut onaylanmış Erişim Noktalarını veya cihazlarını parazite neden olabilecek standart dışı, yetkisiz cihazları devre dışı bırakma hakkına sahiptir. Bu tür cihazlar önceden haber verilmeden çıkartılabilir. Kablosuz ağların izlenmesi, ESOGÜ BİDB tarafından düzenli olarak yapılmaktadır.
- İnternete kimlik doğrulaması olmayan açık erişim, ESOGÜ BİDB çevresinde kablosuz noktalar yoluyla veya güvenli kablosuz ağdan ayrı olarak sağlanmalıdır.
- ESOGÜ BİDB güvenli kablosuz ağında, yalnızca lisanslı veya açık kaynak kod lisanslı yazılımların kullanılmasına izin verilir.
- Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.
- Kullanıcılar tarafından kurumun tüm internet bant genişliğinin tüketilmesi engellenmelidir.
- Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.
- Kablosuz ağa dahil olan kurum çalışanları için bile erişimler sınırlandırılmalıdır. Sadece internete çıkacak olan kullanıcıların kablosuz ağ üzerinden diğer uygulamaların (ses, güvenlik, mobilite vb) çalıştığı networklere erişimi engellenmeli gerekirse networkler farklı IP aralıkları üzerinde ayarlanmalı, cihaz üzerinde Access Control Listler (Yetki kuralları) oluşturulmalıdır.
- Kablosuz ağ cihazlarına erişim sadece yetkili kişiler tarafından Access Controller, SSH ya da cihaz başında console (konsol) ile yapılmalı, http ve telnet protokolleriyle erişim kapatılmalıdır.
- Yetkili Kullanıcılar, aile üyelerinden bile olsa, giriş bilgilerini ve şifrelerini korumalıdır.
- Kuruluşlar ve kullanıcılar, kablosuz iletişim ağlarını uygulamadan ve kullanmadan önce güvenlik tehditlerini anlamaları gerekir. Aşağıda açıklanan tehditler, genel olarak kablosuz ağ cihazları ile ilgili olabilecek tehditlerdir.

- Denial of Service - Saldırgan, kablosuz ağların veya ağ aygıtlarının normal kullanımını veya yönetimini engeller veya sınırlar.
- Dinleme - Saldırgan, kimlik doğrulama kimlik bilgileri de dahil olmak üzere kablosuz ağları veri için pasif olarak izler.
- Man-in-the-Middle - Saldırgan, kablosuz istemciler ve AP'ler arasındaki iletişimleri aktif olarak engeller, böylece kimlik doğrulama kimlik bilgileri ve veriler elde edilir.
- Masquerading - Saldırgan, yetkili bir kullanıcıyı taklit eder ve kablosuz ağlara belirli yetkisiz ayrıcalıklar kazandırır.
- İleti Değişikliği - Saldırgan, kablosuz ağlar yoluyla gönderilen meşru bir iletiyi silerek, ekleyerek, değiştirerek veya yeniden sıralamayla değiştirir
- Mesaj Yeniden Oynatma - Saldırgan, kablosuz ağlar vasıtasıyla iletimleri pasif olarak izler ve mesajı tekrar gönderir; saldırgan meşru bir kullanıcıymış gibi davranıyor.
- Trafik Analizi - Saldırgan, iletişim modellerini ve katılımcılarını belirlemek için kablosuz ağlar vasıtasıyla iletimleri pasif olarak izler.
- Fiziksel olarak Tampered – AP'nin (Access Point – Erişim Noktası) antenindeki değişikliklerden veya AP başka bir yere taşınırsa, şifreler donanımdan alınabilir. Bu, saldırganın lehine olan sinyal gücünü artırır.

6. Yaptırım

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır.

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

7. İlgili Dokümanlar

PR.12 - OLAY İHLAL YÖNETİM PROSEDÜRÜ

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI