1. AMAÇ

Ağ ve Sistemlerin Güvenli İşletimi Prosedürü'nde, üniversite ağ ve sistemlerinin işletimi (kurulum, konfigürasyon, ağa dahil etme, yönetim) sırasında uyulması gereken güvenlik kurallarının ve adımlarının belirlenmesi amaçlanmaktadır.

2. KAPSAM

Bu prosedür, Üniversite ana sisteminde bulunan ağ ve sistemlerin yönetimi ile ilgili standartların belirlenmesi ve risklerin minimuma indirgenmesi amacıyla hazırlanmıştır. Prosedürde bahsi geçen standartlar, ağ ve sistemlerin yönetiminden sorumlu bütün idari kullanıcılar ve dış hizmet çalışanları için geçerlidir.

3. REFERANSLAR

3.1 Uzaktan Erişim Prosedürü

3.2 Konfigürasyon Yönetimi Prosedürü

3.3 Kullanıcı Erişim Yönetimi, Yetkilendirme ve Hesap Yönetimi Prosedürü

3.4 Değişiklik & Versiyon Yönetimi Prosedürü

3.5 Güvenli Yazılım Geliştirme Prosedürü

3.6 BT Fiziksel Çevresel Güvenlik Prosedürü

3.7 Veri Yedekleme Prosedürü

3.8 BT Minimum Güvenlik Standardı

3.9 YÖK Öğrenci Disiplin Yönetmeliği

3.10 Koç Üniversitesi İdari Personel Yönetmeliği

3.11 COBIT.2019 kapsamında "Süreç, Organizasyonel Yapılar, Bilgi Akışları ve Varlıkları, İnsanlar, Beceriler ve Etkinlikler, Politikalar ve Prosedürler, Kültür, Etik ve Davranış, Hizmetler, Altyapı ve Uygulamalar" yönetişim bileşenlerinin ilgili yönetişim ve yönetim hedefine uygulanabilecek her biri.

3.12 ISO 27000:2018 Bilgi Güvenliği yönetim standartları ailesi tamamı.

3.13 SANS-CIS kontrolleri En yaygın ve tehlikeli saldırıları durdurmak için belirli ve uygulanabilir yollar sağlayan, siber güvenlik eylemler dizisidir.

3.14 5651: İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

3.15 6698: Kişisel Verilerin Korunması Kanunu

3.16 4857: İş Kanunu

3.17 2547: YÖK Kanunu

4. SORUMLULUKLAR

4.1 Prosedürün yayına hazırlanmasından, onaylanmasından, yayımlanıp devreye alınmasından, iyileştirme takibinin yapılmasından, ağ ve sistemlerin güvenli işletilme standartlarının uygulandığının kontrol edilmesinden Bilgi Teknolojileri Direktörlüğü sorumludur.

5. TANIMLAR

5.1 Üniversite (KU): Koç Üniversitesi

5.2 Rektör: Koç Üniversitesi Rektörü

5.3 Prosedür: Ağ ve Sistemlerin Güvenli İşletimi Prosedürü

5.4 BT: Bilgi Teknolojileri

5.5 IP(Internet Protokol): Bağlı cihazların, ağ üzerinden birbirleri ile veri alışverişi yapmak için kullandıkları adres.

5.6 DHCP sunucusu: Ağ cihazlarına IP adresi, ağ geçidi gibi gereksinimleri sağlayan DHCP protokolünün otomatik olarak bu işlemi yerine getirmesini sağlayan sistem.

5.7 SNMP: Cihaz üzerindeki sıcaklıktan, cihaza bağlı kullanıcılara, internet bağlantı hızından sistem çalışma süresine kadar çeşitli bilgileri denetlemek amacıyla tasarlanmış Basit Ağ Yönetim Protokolü.

5.8 Güvenlik Duvarı: Bir kural listesine bağlı olarak ağa gelen giden paket trafiğini kontrol eden yazılım veya donanım tabanlı ağ güvenliği sistemidir.

5.9 IDS : Saldırı Tespit Sistemi

5.10 IPS : Saldırı Engelleme Sistemi

5.11 DMZ : Üniversiteye ait internet üzerinden doğrudan erişilebilen sistemlerin konumlandırıldığı, ek güvenlik önlemleri ile korunan izole segment.

5.12 NAC(Network Authentication Control): Ağ Erişim Kontrol

6. TEMEL PRENSİPLER

6.1 Bu prosedür ve bağlantılı diğer yönerge ve prosedürlerin ihlal edilmesi veya ihlal edilmesine sebep olunması halinde KU İdari personeli için 4857 Sayılı İş Kanunu ve Koç Üniversitesi İdari Personel

Yönetmeliği, KU Akademik personel için 2547 Sayılı YÖK Kanunu, öğrenciler için YÖK Öğrenci Disiplin Yönetmeliği işletilmektedir.

6.2 Bu prosedüre dair tüm istisnalar ancak Bilgi Güvenliği Komitesi onayı ile uygulanmaktadır.

6.3 Yerel iletişim ağı altyapısı ile ilgili kablolama, aktif cihazlar (Router, Switch, Access Point vb.), istasyonlar, kabinler gibi detayların da yer aldığı topoloji hazırlanmakta ve güncel tutulmaktadır.

6.4 Tüm ağ yönetim yetkileri (kablolama ve aktif cihaz erişim yetkileri gibi) bir süreç dâhilinde belirlenmekte ve kontrol edilmektedir.

6.5 Kablolamalar endüstri standartlarına uygun şekilde yapılmakta, gerçekleştirilecek kapasite ve kullanıcı artışları ve güvenlik gereksinimleri göz önünde bulundurularak kablolama ihtiyaçları belirlenmektedir.

6.6 Yerel ağa izinsiz erişimler kısıtlanır, dış kaynak erişimleri kontrol altında tutulmaktadır. Sadece yetkili ve tanımlı cihazların Üniversite ağına erişmesi amacıyla ağ erişim kontrolü uygulanmaktadır.

6.7 IP adresi kullanımları Yazılım Geliştirme ve BT Operasyon denetimi altında yapılmaktadır. İzinsiz IP adresi kullanımı engellenmektedir.

6.8 Bilgi teknolojileri alt yapı cihazları, ağ ve sunucu cihazları dâhil olmak üzere aktif cihazların konuşlandırılacağı istasyon, kabin, sistem odası vb. yerlerin güvenliği BT Fiziksel Çevresel Güvenlik Prosedürü'ne uygun olarak sağlanmaktadır.

6.9 Trafiğin dinlenmesine ve kullanıcı/şifre bilgilerin elde edilmesine sebep olabilen Hub cihazları yerel ağlarda kullanılmamaktadır.

6.10 Yerel iletişim ağları için performans ve kapasite yönetimi süreçleri yürütülmekte ve altyapının erişilebilirliği izlenmektedir.

6.11 Periyodik olarak (en az yılda 1 kez) zafiyet analizi ve sızma testleri yaptırılmaktadır.

6.12 Güvenilir ağlar arasında kurulan bağlantıda Internet ve Telco gibi güvenilmeyen ağlar kullanılıyorsa bütün hassas veri (örneğin; Gizli ve Kısıtlı Bilgi) şifrelenmektedir.

6.13 Ağ elemanlarının izlemesi yalnızca Yazılım Geliştirme ve BT Operasyon ekibi tarafından tarafından yapılabilmektedir.

6.14 Gerek kendi kurumsal ağı gerek dış ağlardan gelebilecek tehditler için gerekli ağ güvenlik kontrol sistemleri tesis edilmektedir. Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınmaktadır.

6.15 Websitesi gibi üzerinden doğrudan erişilebilen sistemler DMZ segmentinde bulundurulmaktadır.

6.16 İç ağdan gelebilecek tehditlerin etkisini azaltmak ve Üniversite iç ağının farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere Üniversite iç ağındaki her bir servise ilişkin trafiğin yalnızca kendisi için gerekli olan ağ segmentlerine ulaşmasını sağlayacak şekilde Üniversite iç ağı alt bölümlere ayrılmaktadır. Kritik ağ bileşenleri (sunucular vb.) standart ağdan ayrılmakta ve bu ağ bileşenleri özelinde ek erişim sınırlandırmaları gerçekleştirilmektedir.

6.17 Dış ağı ve iç ağı arasındaki trafiği kontrol altında tutmak için gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan güvenlik duvarı çözümleri ile saldırıları tespit edebilecek (IDS) ve önleyebilecek (IPS) günün teknolojisine uygun sistemler kullanılmaktadır.

6.18 Hassas veya sır kapsamındaki verilere sahip sistemlerin özel iç ağda bulunmakta ve hiçbir şekilde doğrudan internetten erişilemiyor olması sağlanmaktadır.

6.19 Merkezi yetkilendirme ağ cihazlarına genel yönetimsel erişim için kullanılmaktadır. (örneğin; TACACS+, Güvenli LDAP) Yerel hesaplar merkezi erişim sisteminin erişilemez olduğu acil durumlarda kullanılabilmektedir.

6.20 Bütün ağ donanımları Yazılım Geliştirme ve BT Operasyon yöneticisi tarafından onaylanmaktadır. Yazılım Geliştirme ve BT Operasyon ekibi kendi yönetimindeki bütün ağ cihazlarının temel yapılandırma standartları sürdürülmektedir.

6.21 Bütün ağ cihazlarının bakımı uygulanabilir yapılandırma standartlarına uygun olarak yapılmaktadır.

6.22 İç ağ ve Internet arasındaki bütün trafik Üniversite tarafından yönetilen güvenlik duvarı üzerinden geçmektedir.

6.23 İç ağa sadece yetkilendirilmiş cihazların bağlanabilmesi sağlanmaktadır.

6.24 İç segmentte yer alan kritik ağ segmentlerine erişim ek güvenlik önlemleri alınarak sağlanmaktadır. Kablolu/Kablosuz intranet bağlantılarında teknik altyapının imkan verdiği fiziksel lokasyonlarda NAC mekanizmasından geçirilirek son kullanıcılara ağa erişim izni verilmektedir.

6.25 Dış bağlantı için yetkiler servis sahibi onayı ile servis operatörü tarafından verilmektedir. Dış bağlantılar kayıt altına alınmakta ve izlenmektedir. Dış bağlantılar periyodik olarak altı ayda bir süreç sahibi ile Bilgi Güvenliği ekibi tarafından Dış Bağlantılar Kontrol Listesi'ne göre gözden geçirilmektedir.

6.26 Uzaktan erişimler, Uzaktan Erişim Prosedürü'ne uyumlu olacak şekilde yapılmaktadır.

6.27 Uzak teşhis ve yapılandırma ile portlar yetkisiz ağ erişime karşı korunmaktadır.

6.28 Ağda bulunan tüm sistemlerin saat ve takvimleri otomatik olarak zaman sunucusu üzerinden senkronize edilmektedir.

6.29 Ağ sunucu/sistem/cihazları fiziksel olarak güvenli bir lokasyonda bulunmaktadır.

7. YÖNTEM

7.1 IP Adres Bloklarının Dağıtımı

7.1.1 Private IP adres blokları Yazılım Geliştirme ve BT Operasyon ekibi tarafından verilmektedir. Kayıtlı (registered) adres bloğu hazırda mevcuttur.

7.1.2 IP Adres Bloğu Tahsis Kuralları

7.1.2.1 Intranette veya Internette kullanılan tüm IP bloklarının kullanımına ilişkin IP tahsisi Yazılım Geliştirme ve BT Operasyon ekibi tarafından yapılmaktadır.

7.1.2.2 Tahsis edilen IP bloklarının birim içerisindeki dağılımı değiştiğinde, tek bir konsol üzerinden kayıtlar takip edilmektedir.

7.1.2.3 Ağ güvenlik taramaları Yazılım Geliştirme ve BT Operasyon ve Bilgi Güvenliği ekibi koordinasyonunda gerçekleştirilmektedir.

7.1.2.4 Ağ üzerinde aktif veya pasif olarak cihaz tespiti, ağ trafiğinin izlenmesi faaliyetleri için kullanılan yazılımlar yetkili kişiler (servis sahibi & operatörü) tarafından kullanılabilmektedir. 3. taraf firmalar ancak Bilgi Güvenliği Yöneticisi ve Yazılım Geliştirme ve BT Operasyon Yöneticisi onayı ile Tedarikçi Yönetimi Prosedürü'ne uygun olarak faaliyetlerde bulunabilmektedir.

7.1.2.5 Intranette son kullanıcı IP adres atamaları, Domain Sunucuları ile entegre olarak çalışan DHCP sunucuları ile dağıtılmaktadır.

7.1.2.6 Ziyaretçi bağlantılarında kullanılmak üzere bir VLAN belirlenmektedir. Belirlenen VLAN üzerinden ziyaretçilere kimlik doğrulaması yapıldıktan sonra atama işlemi sağlanmakta ve bu VLAN sadece internete erişim sağlanabilen izole bir VLAN olarak yapılandırılmaktadır. Yasal gereksinimlere uygun şekilde loglama gerçekleştirilmektedir.

7.1.2.7 KU mensupları, internet (bir tarayıcı ile erişilen) kullanımını kendisine has verilen kullanıcı adı ve şifresi ile veya başka doğrulama yöntemleri sonrası içerik filtreleme mekanizmasından geçerek yapabilmektedir.

7.2 Ağ Cihazlarının ve Sunucuların İşletimi

7.2.1 Ağ Cihazları ve Sunucuların Kurulumu Adımları

7.2.1.1 Yeni bir sistem (sunucu, ağ cihazı, v.b.) kurulacağı veya daha önceden kurulumu yapılmış bir sistem üzerinde topoloji değişikliği, sunucu/sistem/cihaz değişimi, yazılım değişikliği v.b. önemli bir değişiklik yapılacağında aşağıdaki adımlar uygulanmaktadır.

7.2.1.1.1 Talebi yapan kişi/birim ihtiyacı olan sunucu/sistem/cihaz ihtiyacını Yazılım Geliştirme ve BT Operasyon ekibine iletmektedir.

7.2.1.1.2 Yazılım Geliştirme ve BT Operasyon ekibi ve Bilgi Güvenliği Yöneticisi kurulacak yapıya ilişkin güvenlik yapılandırması, veri şifreleme ihtiyaçları, topoloji ve güvenlik açığı kapsamında bilgi güvenliği değerlendirmesini yapmaktadır.

7.2.1.1.3 Bilgi güvenliğinde sorun oluşması halinde red bilgisini, sorun oluşmaması halinde aksiyon alınacağı talebi yapana iletilmektedir.

7.2.1.1.4 Yeni sunucu/sistem/cihaz servis sahibi tarafından bilgi güvenliği değerlendirmesine uygun olarak (BT Minimum Security Standarts - BT Minimum Güvenlik Standardında belirtildiği üzere) kurulmakta ve gerekli tanımlamalar yapılmaktadır. BT minimum güvenlik standartlarını karşılamayan cihazların, ilgili eksiklikler giderilene kadar, KU ağına erişimi geçici olarak kapatılmaktadır.

7.2.1.1.5 Kurulan sunucu/sistem/cihaz IP adres bilgisi, gerekiyorsa domain adı ilgili tabloya ve topoloji diyagramına işlenmektedir.

7.2.1.2 Ağ sunucu/sistem/cihaz kurulumu sırasında, aşağıdaki kurallara uyulmaktadır.

7.2.1.2.1 Sunucu/sistem/cihaz kullanıma ihtiyaç duyulmayan uygulama ve servisler kapatılmaktadır.

7.2.1.2.2 Sunucu/sistem/cihaz kullanıcıları, Yazılım Geliştirme ve BT Operasyon ekibinden erişim hakkı talep etmekte ve uygun görülmesi durumunda erişim hakkı verilmektedir.

7.2.1.2.3 Yönetici şifreleri, SNMP tanımları ve benzeri "fabrika ayarları" (default settings) başlangıç ayarlarında bırakılmamaktadır. Varsayılan yönetici şifreleri iptal edilmekte veya değiştirilmektedir.

7.2.1.2.4 Ağlarda mutlaka segmentasyon uygulanmaktadır.

7.2.1.3 Ağlarda segmentasyon uygulanırken şu kurallar dikkate alınmaktadır.

7.2.1.3.1 Segmentasyon oluşturulmadan önce ihtiyaç duyulması halinde güvenlik değerlendirmesi Yazılım Geliştirme ve BT Operasyon Yöneticisi ve Bilgi Güvenliği Yöneticisi tarafından yapılmaktadır.

7.2.1.3.2 DMZ segmenti dışarıdan erişilen KU servisleri için kullanılmaktadır. Üniversite'nin yerel ağındaki sistemlerden ayrılmaktadır.

7.2.1.3.3 Sunucular ile son kullanıcılar farklı segmentlerde bulundurulmaktadır.

7.2.1.3.4 Farklı işlevleri yürüten iş sistemleri, farklı segmentlerde bulundurulmaktadır. Tüm sistemler güvenlik sistemlerinin arkasında konumlandırılmaktadır.

7.2.1.4 Eğer var ise; uzak bölgedeki personelin sunucu/sistem/cihaz erişim hakları yalnızca iş ihtiyaçları dahilinde verilmektedir.

7.2.2 Ağ Sunucu/Sistem/Cihazlarının Ağa Dahil Edilmesi

7.2.2.1 Ağ sunucu/sistem/cihazlarının ağa dahil edilmesi öncesinde, gerekli konfigürasyonların yapıldığı kontrol edilmektedir. Gereken tüm yazılımların (örneğin yamaların ve anti-virüs yazılımlarının) güncel sürümlerinin yüklendiğinden emin olunmaktadır.

7.2.2.2 Ağ sunucu/sistem/cihazlarının ağa dahil edilmesi başka sunucu/sistem/cihazlarını etkileyecekse, Yazılım Geliştirme ve BT Operasyon Yöneticisi, takım liderleri ile iletişime geçilmekte ve sürecin yürütülmesi için koordinasyonu sağlanmaktadır.

7.2.3 Ağ Sunucu/Sistem/Cihazlarının Konfigürasyon Değişimi Kuralları

7.2.3.1 Ağ sunucu/sistem/cihazlarındaki konfigürasyon değişiklikleri Konfigürasyon Yönetimi Prosedürü'ne uygun olarak gerçekleştirilmektedir.

7.2.4 Ağ Sunucu/Sistem/Cihazlarının Yönetimi

7.2.4.1 Ağ sunucu/sistem/cihazlarının yönetimi, servis sahibi & operatörleri tarafından Kullanıcı Erişim Yönetimi, Yetkilendirme ve Hesap Yönetimi Prosedürü'ne uygun olarak yapılmaktadır. Servis sahibi & operatörleri bu yetkilerini başka çalışanlara devredilmemektedir.

7.2.4.2 Servis sahibi & operatörleri bilgileri (parola, vb.) başkaları ile paylaşılmamaktadır.

7.2.4.3 Yönetim işlemlerinin güvenli protokollerle yapılması (örn. telnet yerine SSH) öncelikle tercih edilmektedir.

7.2.4.4 Sunucu/sistem/cihazların yönetimine ilişkin işlemlerin kaydedilmesi için gerekli audit log konfigürasyonu yapılmaktadır. Bu kayıtlar en az bir yıl süre ile saklanmaktadır.

7.2.4.5 Sunucu/sistem/cihazların sağladığı işlevlerden yararlanacak tarafların taleplerinin nasıl karşılanacağı (talep iletme biçimleri, talep sahibinin doğrulanması, vb.) ve bu amaçla yapılacak yönetim adımlarında hangi mekanizmaların işletileceğini tarif etmek ve uygulamak Yazılım Geliştirme ve BT Operasyon ekibinin sorumluluğundadır.

7.2.4.6 Sunucu/sistem/cihazların yazılım ve donanım niteliklerinin değiştirilmesi gerektiğinde, Konfigürasyon Yönetimi Prosedürü'ne ve Değişiklik & Versiyon Yönetimi Prosedürü'ne uygun olarak işlem yapılmaktadır.

7.2.4.7 Sunucu/sistem/cihazların bakım-onarım faaliyetlerinin ilgili KU çalışanı refakatinde yetkin ekipler tarafından gerçekleştirilmesi ve devre dışı bırakılması gerektiğinde BT Fiziksel Çevresel Güvenlik Prosedürü'ne uygun olarak işlem yapılması gerekmektedir.

7.2.4.8 Kullanılmayan portlar devre dışı bırakılmaktadır.

7.2.4.9 Kabinler ve kabinlerin bulunduğu odalar, BT Fiziksel Çevresel Güvenlik Prosedürü'ne uygun olarak korunmaktadır.

7.2.4.10 Yedekleme gereken durumlarda sunucu/sistem/cihazlarda Veri Yedekleme Prosedürü'ne göre işlemler yürütülmektedir.

7.3 Güvenlik Sistemlerinin İşletimi

7.3.1 KU ağ yapısındaki istemci ve sunucu makinalarında kullanılan Güvenlik Sistemlerinin yönetimi Yazılım Geliştirme ve BT Operasyon ekibi koordinasyonunda ve gözetiminde, Bilgi Güvenliği Ekibi'nin bilgisi dahilinde yetkilendirilmiş servis sahibi & operatörleri tarafından gerçekleştirilmektedir.

7.3.2 Güvenlik Sistemlerinin Kullanılması ile İlgili Kurallar

7.3.2.1 KU ağ yapısının güvenliğini sağlamak için güvenlik sistemleri aşağıda belirtilen şekilde kullanılmaktadır:

7.3.2.1.1 Üniversite içindeki tüm istemciler, sunucular ve ağ cihazları güvenlik sistemleri ile korunmaktadır.

7.3.2.1.2 İstemcilerin Internet çıkışı mutlaka güvenlik duvarı ve içerik filtreleme sistemleri(sadece ziyaretçiler için) üzerinden geçirilerek yapılmaktadır.

7.3.2.2 Uzak Bağlantı Kuralları:

7.3.2.2.1 Sistem yöneticilerinin uzaktan çalışması gereken zamanlarda, Üniversite ağına VPN hizmeti ile bağlanılmaktadır. VPN ile ağa dahil olunmadan VPN üzerindeki konfigürasyonlarla hangi kullanıcının hangi role dahil olduğu tespit edilmekte ve bu role göre kullanıcıların erişebilecekleri yerlere (IP, port vb.) izin verilmektedir.

7.3.2.2.2 Bilgi Güvenliği Yöneticisi ve Yazılım Geliştirme ve BT Operasyon yöneticisi tarafından yetkilendirilen personel dışında son kullanıcıların VPN ile Üniversite ağına bağlandıklarında telnet, SSH, remote desktop vb. hakları yoktur. Yalnızca ihtiyaç olunan sunucuya gereken port(lar) ile bağlanılmaktadır.

7.3.2.2.3 Uzak konsol, kabuk (shell) veya yönetici ara yüzün erişimi için Telnet, http ve diğer güvenli olmayan protokollerin kullanımına izin verilmemektedir.

7.3.2.3 Güvenlik Duvarı Güvenlik Kuralları:

7.3.2.3.1 Bütün bağlantılar genel/özel (public/private) anahtar algoritmaları ile yetkilendirilmekte ve şifrelenmektedir.

7.3.2.3.2 Yönetici konsol bağlantıları için token ile üretilmiş şifre veya güçlü kullanıcı adı/şifre, çift faktörlü kimlik doğrulama ve yetkilendirme için kullanılmaktadır. Bu süreç Kullanıcı Erişim Yönetimi, Yetkilendirme ve Hesap Yönetimi Prosedürü'ne uygun olarak yönetilmektedir.

7.3.2.3.3 Bütün yönetici aktiviteleri log sunucusu üzerine loglanmalı ve bu yöneticilerin hiçbirisinin bu loglar üzerinde düzenleme hakkı bulunmamaktadır.

7.3.2.3.4 30 dakika kullanılamayan uzaktan erişim bağlantıları kapatılmaktadır.

7.3.2.3.5 Güvenlik duvarı yönetici sayısı bağlantıları minimumda tutmak için kısıtlanmaktadır. Günlük operasyonel görevler bazı hesaplara atanmakta, bu hesapların yönetici yetkileri bulunmamaktadır.

7.3.2.4 Güvenlik Duvarı Konfigürasyon Kuralları:

7.3.2.4.1 Güvenlik duvarının arkasında duran bütün cihazlar, güvenlik duvarı üzerinde bulunan Ethernet portları üzerinden kendi güvenlik seviyelerine göre segmentlere ayrılmaktadır. Dış Segment: Güvenlik duvarı kapsamının dışında kalan bölümler.

İç Segment: Güvenlik duvarı arkasında kalan güvenli bölüm.

7.3.2.4.2 Yalnızca herkese açık olan servisler dış segmentten erişilebilir olmalı. Diğer bütün trafik engellenmektedir.

7.3.2.4.3 Internet güvenlik duvarı yetkili giden trafik için bütün iç IP adreslerini kendi dış arabirim IP adresine dönüştürmektedir. Özgün IP adresi olması gereken istisna durumlarda, duruma mahsus olmak üzere Yazılım Geliştirme ve BT Operasyon Yöneticisi onayı ile izin verilmektedir.

7.3.2.4.4 SNMP erişimi gerekli ise, bu yalnızca belirli yönetim sunucularına salt okunur olarak etkinleştirilebilmektedir.

7.3.2.4.5 SNMP tabanlı alarm olayları belirli yönetim sunucularına iletilmektedir. (SNMP Trap)

7.3.2.4.6 Bütün bağlantılar hakkındaki izin ve red kayıtları (log), kayıt sunucusuna gönderilmektedir. Bu kayıtları Bilgi Güvenliği Yöneticisi izleyebilmektedir.

7.3.2.4.7 Kural setlerini yalnızca yetkilendirilmiş kullanıcılar (servis sahibi & operatörü) yapılandırabilmektedir.

7.3.2.5 NAC Kurulumu ve Devreye Alma

7.3.2.5.1 Cihaz, yerel ağda "Out-of-band" mimaride konumlandırılmaktadır. Bu sayede trafik sürekli olarak NAC cihazı üzerinden geçmemektedir.

7.3.2.5.2 Kullanıcı ve cihaz profilleri yaratılmaktadır. Buna yönelik olarak bir IP ve MAC listesi oluşturulmaktadır. Bu kullanıcı ve cihaz profilleri için erişim politikaları belirlenmektedir.

7.3.2.5.3 Kullanıcı Erişim Yönetimi, Yetkilendirme ve Hesap Yönetimi Prosedürü'nde yer alan farklı kullanıcı profillerine göre farklı kimlik doğrulama ve erişim politikaları uygulanmaktadır.

7.3.2.5.4 Üniversite kullanıcıları için bilgisayarlar üzerinde uygulanması gereken bilgi güvenliği standartları NAC sistemi üzerinde tanımlanmaktadır. Kontrolün bu sistem tarafından yapılması sağlanmaktadır.

7.3.2.5.5 Cihaz üzerinde Https veya SSH yöntemi ile erişim belirli IP'lerden olacak şekilde sınırlandırılmaktadır. Telnet, Http, FTP gibi güvensiz erişim yöntemleri ve gereksiz servisler kapatılmaktadır.

7.3.2.6 NAC İşletim ve Bakımı

7.3.2.6.1 Yeni oluşabilecek tehditlere karşı, sistemin yazılım güncellemeleri takip edilmekte, incelendikten sonra uygulanmaktadır.

7.3.2.6.2 Sistemin event logları merkezi log sistemine aktarılmaktadır.

7.3.2.6.3 Performans değerleri (CPU, RAM vb.), trafik yoğunluğu, atak durumlarının sürekli olarak izlenmesine yönelik planlama yapılmaktadır. Mail, SNMP trap ve benzeri yöntemler ile çevrimiçi alarm mekanizması aktif edilmektedir.

7.3.2.6.4 NAC kontrollerinden geçemeyen kullanıcılar günlük olarak sistem üzerinden çekilen raporlar ile kontrol edilmektedir.

7.3.2.6.5 Anti-virüs, uygulama, güvenlik açıkları gibi kontrollerin yapılmasını sağlayan imza güncelleme özelliği otomatik modda çalıştırılmaktadır.

7.3.2.6.6 Üniversite bilgisayarları üzerinde kurulması gereken ajan veya uygulanması gereken tanımlamaların Active Directory üzerinden Group Policy güncellemeleriyle sağlanması gerekmektedir.

7.3.3 Güvenlik Sistemlerinin İşletilmesi

7.3.3.1 Güvenlik sistemlerinin yönetiminde aşağıdaki temel kurallar işletilmektedir:

7.3.3.1.1 Güvenlik sistemlerinin operasyonu, Yazılım Geliştirme ve BT Operasyon ekibi tarafından belirlenen süreçler doğrultusunda yürütülmektedir.

7.3.3.1.2 Üniversite'ye hizmet veren firmalar, doğrudan güvenlik düzenlemesi talebinde bulunamamaktadırlar. Talepler firma'nın hizmet verdiği ilgili birim tarafından iletilmektedir.

7.3.3.1.3 Güvenlik duvarında kural düzenlemesi ve benzeri talepler iletildiğinde, istenen kural parametreleri (IP adres, port numarası, vb.), gerekçesi, süresi ve gerek duyulacak diğer bilgiler eksiksiz olarak iletilmektedir.

7.3.3.1.4 Gelen kural talepleri servis sahibi tarafından onaylanmakta ve servis operatörü tarafından devreye alınmaktadır.

7.3.3.1.5 Standart dışı gelen kural talepleri Bilgi Güvenliği Yöneticisi onayı sonrası servis sahibi tarafından onaylanmakta ve servis operatörü tarafından devreye alınmaktadır.

7.3.3.1.6 Birimlerden gelen taleplere istinaden yapılan düzenlemeler, ilgili birime talebin geldiği kanal ile bildirilmektedir.

7.3.3.1.7 Üniversite altyapısında gerekli iyileştirmelerin planlanabilmesi için, kişi(ler) altyapıda öngördükleri değişimleri (kapasiteler, topolojiler, vb.) talep edebilmektedirler. Alınan talepler Bilgi Güvenliği Yöneticisi ve Yazılım Geliştirme ve BT Operasyon yöneticisi tarafından değerlendirilerek, kabul veya reddedilmektedir.

7.3.3.1.8 Dış hizmet alınan firmalar ile yapılacak çalışmalarda trafiğin kaynaklanacağı IP adres bilgileri alınmakta, bu kaynak IP adreslerinden gelmeyen trafik kabul edilmemekte ve yönlendirilmemektedir.

7.3.3.1.9 Güvenlik sistemleri üzerinde 2 yönlü (hem içeri doğru akan trafik için hem de dışarı doğru akan trafik için) filtreleme yapılmaktadır.

7.4 İşletim Sistemlerinin İşletimi

7.4.1 Sistemler üzerindeki işletim sistemlerinin kurulumu, yapılandırması ve yönetimi Yazılım Geliştirme ve BT Operasyon ekibi tarafından yapılmakta/koordine edilmektedir.

7.4.2 Üniversite tarafından kurulan engelleme/kontrol mekanizmaları devre dışı bırakılamamaktadır.

7.4.3 Standart son kullanıcı uygulamaları haricinde talep edilen uygulamaların yüklenmesi için talep yönetim sistemi üzerinden süreç başlatılmaktadır. Talep sahibinin yöneticisinden ve Bilgi Güvenliği yöneticisinden güvenlik değerlendirmesi yapılarak onay alındıktan sonra kabul veya reddedilmektedir.

8. EKLER ve KAYITLAR

EK-1 Dış Bağlantılar Kontrol Listesi

EK-2 Minimum Güvenlik Standartları

9. GÖZDEN GEÇİRME

Bu dokümanı gözden geçirme ve güncelleştirme sorumluluğu Bilgi Teknolojileri Direktörlüğü'ne aittir. Gözden geçirme en az yılda 1 defa yapılır. Gerekli görüldüğü zaman ve durumlarda dokümanın da revize edilmesi gereklidir.

10. DEĞİŞİKLİK/ DAĞITIM/ ONAY TABLOSU

Değişen sayfa	Tarih	Değişiklik	Değişikliği yapan
11	03.08.2021	Minimum Güvenlik Standartları listesi ek olarak eklenmiştir.	Ertuğrul Doğan
Dağıtım (İlgili Bölümler)			
Tüm Koç Üniversitesi			