1. AMAÇ

Bu talimatın amacı, Kerevitaş Gıda San. ve Tic. A.Ş.'ye ait sistemlerin siber tehditlere karşı güvenliğinin sağlanması için kullanılan yaklaşım ve çözümleri tanımlamaktır.

2. KAPSAM

Bu prosedür Kerevitaş Gıda San. ve Tic. A.Ş.'ye ait tüm sistemleri kapsar.

3. GÖREV, YETKİ VE SORUMLULUKLAR

R (Responsible)	İşi Yapan Sorumlu kişidir, her satırda ve sadece bir tane R bulunmalıdır.	**C (Consulted)**	Danışılan kişidir.
A (Accountable)	İşin Yapıldığını Onaylayan kişidir, her satırda bir tane A bulunmalıdır. İşin bitirilmesi konusunda ilk soru yöneltilecek kişidir.	**I (Informed)**	Bilgilendirilen kişidir.

Roller Sorumluluklar	**Bilgi Güvenliği Direktörü**	**Uygulama/Sistem Sahibi Yöneticisi**	**Yardım Masası**	**Siber Güvenlik Direktörlüğü**	**Bilgi Güvenliği Kurulu**
Risk analizinin yapılması	R			C	A
Risk analiz sonucuna göre çözüm seçimi	I	R		AR	I
Çözümün devreye alınmasının onayı			I	AR	RI
Çözümün kullanım politikalarının belirlenmesi	AR			C	I
Çözümün devreye alınıp işletilmesi	I	R	I	A	I

4. UYGULAMA

Kerevitaş Gıda San. ve Tic. A.Ş, siber güvenliği aşağıdaki alanlarda değerlendirir. Katmanlı güvenlik yaklaşımını kabul eder. İlgili alanlarda kullandığı çözümler aşağıda belirtilmiştir.

1. Uç Nokta güvenliği
2. Veri Güvenliği
3. Zafiyet Yönetimi
4. Uygulama Güvenliği
5. Güvenli Uzak Erişim
6. İzleme

4.1.Uç Nokta Güvenliği

Uç nokta güvenliği, şirket ağına bağlı olan bilgisayarları, dizüstüleri, tabletleri ve mobil cihazları siber tehditlere karşı korumak için kullanılan bir çözümdür. Uç nokta güvenliği, cihazların fiziksel kaybına veya çalınmasına, ağa erişen kötü amaçlı yazılımlara veya yetkisiz kişilere karşı savunma sağlar. Uç nokta güvenliği, ağ güvenliğinin önemli bir parçasıdır ve veri hırsızlığı, fidye yazılımı, kimlik avı ve diğer siber saldırı risklerini azaltmaya yardımcı olur.

1. Symantec EndPoint Security ve Microsoft Defender
   Kullanıcı bilgisayar ve sunucularda zararlı yazılımlara karşı koruma sağlar.
2. Forcepoint URL Filter
   Kullanıcıların güvenli internet erişimlerini sağlar.
3. Windows Defender Firewall
   Ağ seviyesinde kullanıcı bilgisayarlarına yapılacak saldırıları engeller.
4. Windows Defender ATP - EDR
   İleri seviye zararlıları belirlemede kullanılır.
5. Phishing – Training
   Oltalama saldırılarına karşı çalışanların farkındalığını artırmak ve ölçmek için kullanılır.
6. Mail güvenliği
   Mail güvenliği için MS O365 advanced security paketi kullanılır.
7. Kimlik güvenliği
   Kimlik güvenliği için MS O365 advanced security paketi kullanılır.

4.2.Veri Güvenliği

Veri güvenliği, bilgisayar sistemleri, ağlar, veritabanları ve diğer dijital ortamlarda saklanan veya iletilen her türlü verinin yetkisiz erişim, kullanım, değiştirme, ifşa, kayıp veya imhadan korunmasıdır. Veri güvenliği, verilerin bütünlüğünü, gizliliğini ve kullanılabilirliğini sağlamak için teknolojik, kurumsal ve yasal önlemleri içerir. Veri güvenliği, siber saldırılar, doğal afetler, insan hatası veya kasıt gibi çeşitli tehditlere karşı verilerin korunmasını amaçlar.

1. Symantec DLP
   Bilgi Güvenliği Kurulunun belirlediği kurallara göre veri sızmasını izler.
2. Disk Şifreleme
   Bilgisayarın kaybolması ve çalınması durumunda üzerindeki verilerin korunmasını sağlar.
3. RMS - Right Management System
   Ofis dosyaları ile pdf dosyalarının korunmasını sağlar.
4. SecureFileTransfer
   Kullanıcıların kurum dışından güvenli dosya alması ve göndermesi için kullanılır.
5. AIP -Veri sınıflandırma
   Bilgi Güvenliği Kurulunun belirlediği sınıflandırma seviyelerine göre dokümanların sınıflandırılması ve etiketlenmesinde kullanılır
6. Local CA
   Kullanıcıların kurum kablosuz ağına bağlanmasında transparan kimlik doğrulama sağlar ve dışa açık olmayan web uygulamalarının hat güvenliğini sağlar.

4.3.Zafiyet Yönetimi

Zafiyet yönetimi, bilgi sistemlerindeki güvenlik açıklarını tespit etmek, değerlendirmek ve gidermek için yapılan süreçtir. Zafiyet yönetimi, saldırganların sistemlere sızmasını, veri ihlallerine yol açmasını veya hizmet kesintilerine neden olmasını önlemeyi amaçlar. Zafiyet yönetimi, düzenli tarama, risk analizi, yama uygulama ve raporlama gibi adımları içerir.

1. Vulnerability Scanner - Qualys
   Sunuculardaki açıklıkları saldırganlardan önce bulup kapatmak için kullanılır.
2. InsightVM - web zafiyet tarama
   Web uygulamalarındaki açıklıkları saldırganlardan önce bulup kapatmak için kullanılıyor.
3. Fortify Static Source Code Analiz
   Uygulamalardaki zafiyetleri, uygulama canlıya alınmadan önce bulup ilgili zafiyetleri kapatmak için kullanılır.
4. Penetration Testing Service
   Sistemlerin zafiyetleri saldırgan gözüyle profesyonel bir firmaya test ettirilir. Çıkan zafiyetler kapatılır.
5. Hardening -Sechard
   Sunucuların güvenlik seviyelerinin uluslararası CIS (Center of Internet Security) standardına göre iyileştirilmesini sağlar.

4.4.Uygulama Güvenliği

Uygulama güvenliği, web uygulamalarının ve verilerinin siber saldırılardan korunmasını sağlayan bir süreçtir. Uygulama güvenliği, uygulamaların tasarım, geliştirme, kullanım ve test aşamalarında güvenlik açıklarının önlenmesi ve tespit edilmesi için araçlar ve yöntemler içerir. Uygulama güvenliği, gizlilik, bütünlük ve erişilebilirlik gibi temel güvenlik ilkelerini uygulamalara uygular.

1. F5 - WAF, LOAD BALANCER
   Web uygulamalarına yapılacak saldırıları engeller ve birden fazla uygulama sunucusu olan sistemlerde yük dağıtımı yapar.
2. SSL Certificate
   Web uygulamalarına erişimde hat güvenliğini sağlar
3. Microsoft Cloud Apps Security
   Bulut servislerinde kullanıcı hareketlerini izler. Anomalileri belirler.
4. Microsoft Defender for O365
   Microsoft bulut (office 365) ortamında güvenliği sağlar.

4.5.Güvenli Uzak Erişim

Güvenli uzak erişim, çalışanların veya danışmanların şirketin ağ kaynaklarına dışarıdan bağlanabilmesine izin veren bir teknolojidir. Bu teknoloji sayesinde kullanıcılar, evden, seyahatten veya başka bir lokasyondan şirketin sistemlerine erişebilir ve işlerini yapabilirler. Güvenli uzak erişim için genellikle VPN (Virtual Private Network) gibi güvenlik önlemleri alınır ve kullanıcılara kimlik doğrulama yapılarak yetki verilir.

1. Pulse Secure - VPN
   Kullanıcı ve danışmanların şirket dışından şirket ağındaki sistemlere güvenli erişimlerini sağlar.
2. PAM -CyberArk
   Danışmanların sistemler üzerinde yaptıkları işleri kaydeder ve önemli hesapları korur
3. Local CA
   Kullanıcıların kurum kablosuz ağına bağlanmasında transparan kimlik doğrulama sağlar. Ve dışa açık olmayan web uygulamalarının hat güvenliğini sağlar.
4. MFA (Multi Factor Authentication)
   Sistemlere erişimde güçlü kimlik doğrulama sağlar.

4.6. İzleme

Güvenlikte izleme süreci, sistemlerin ve ağların sürekli gözlenmesi, şüpheli veya anormal faaliyetlerin tespit edilmesi ve gerektiğinde müdahale edilmesini içerir. Güvenlik olaylarını erken fark etmek ve analiz etmek için log toplama, SIEM, IDS/IPS gibi araçlardan yararlanılır. Güvenlikte izleme süreci, kurumun güvenlik risklerini azaltmasına, siber saldırılara karşı korumasına ve varsa ihlallerin etkisini minimize etmesine yardımcı olur.

1. SIEM- IBM Qradar, log toplama
   Kritik sistemlerin güvenlik loglarını toplar.
2. Security Operation Center
   7x24 sistemlerin loglarını izler analiz eder ve önemli olanlarını aksiyon alınması için bildirir
3. ThreatMon
   Siber dünyada kuruma ait varlıkları izler.
4. File Audit - DI
   Dosya sunucularında izleme yapar. Dosyaların oluşturulma, silinme değiştirmelerini izler.
5. Azure ATP
   Aktif dizin sunucularının güvenliğini sağlar, kimlik hırsızlıklarını engeller.