BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

T.C.
BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU
Bilgi Teknolojileri Dairesi Başkanlığı

2025 AİLE YILI

Sayı : E-34374171-951.01.09.02-49450

18.09.2025

Konu : Siber Güvenlik Açıklıkları (Erişime Açık Dosya Paylaşım Servisi (SMB))

DOKUR GIDA TURİZM İŞLETMECİLİĞİ VE TİCARET LİMİTED ŞİRKETİNE
KILIÇ ALİ PAŞA MAHALLESİ AKARSU YOKUŞU SK.NO:21A CİHANGİR BEYOĞLU İSTANBUL

Kurumumuz bünyesinde yer alan Ulusal Siber Olaylara Müdahale Merkezi (USOM); ülke kapsamında, yurtiçi ve yurtdışı kaynaklı siber tehditleri tespit etme ve önleme faaliyetleri yürütmektedir. Söz konusu siber güvenlik faaliyetlerine ilişkin olarak yapılan çalışmalar çerçevesinde ilgililere yönelik olarak alarm, uyarı ve duyuru işlemleri de yapılmaktadır.

5809 sayılı Elektronik Haberleşme Kanununun, 60 ıncı maddesinin onbirinci, onikinci ve onüçüncü fıkralarında Bilgi Teknolojileri ve İletişim Kurumu'nun yetkilerine ilişkin olarak şu hükümler yer almaktadır:

(11) "Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır."
(12) "Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum bu fıkrada belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği çerçevesinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir."
(13) "Gerçek kişiler ile özel hukuk ve tüzel kişileri, Kurumun bu maddedeki görevleri ile ilgili taleplerini, tabi oldukları mevzuat hükümlerini gerekçe göstermek suretiyle yerine getirmekten kaçınamazlar. İşletmeciler dışında Kurumun görevleri ile ilgili yükümlülüklerini yerine getirmeyenlere bu maddenin ikinci fıkrasındaki yaptırım uygulanır. (bin liradan bir milyon liraya kadar idarî para cezası) "

Bu çerçevede; tarafınıza tahsisli olan Ek'teki 'IP/URL/ALAN ADI' Listesi'nde belirtilen varlıklarda 'Erişime Açık Dosya Paylaşım Servisi' çalışması kapsamında gerçekleştirilen taramalarda SMB dosya paylaşım servisinin internet erişimine açık olduğu tespit edilmiştir. Bu sistemlerin internet üzerinden erişilebilir olması kritik olup risk teşkil etmektedir. Bu sebeple; gerekli kontrol ve sıkılaştırmaların uygulanmasına müteakip alınan aksiyonlar hakkında USOM'a en geç 15 (on beş) gün içerisinde yazı alt bilgisinde yer alan kep adresi üzerinden veya posta yoluyla yazılı bilgi verilmesi hususunda,

Gereğini rica ederim.

Bu belge, güvenli elektronik imza ile imzalanmıştır.
Doğrulama Kodu: 7B210691-9871-4B76-B206-D41E4CC8EE69 Doğrulama Adresi: https://www.turkiye.gov.tr/btk-ebys

Bilgi Teknolojileri Ve İletişim Kurumu
Eskişehir Yolu 10.Km No:276 Çankaya/Ankara
Tel: 0 312 412 20 00 Faks: 0 312 412 20 80
KEP Adresi : btk@btk.hs01.kep.tr

Bilgi için:. USOM
Birim Sorumlusu

Demet KABASAKAL
Başkan a.
Daire Başkanı V.

Ek: Teknik Ek

19/09/2025
Güvenli Elektronik
İmzalı Aslı ile Aynıdır.
Levent SARIKAYA
Büro Personeli

Bilgi Teknolojileri Ve İletişim Kurumu
Eskişehir Yolu 10.Km No:276 Çankaya/Ankara
Tel: 0 312 412 20 00 Faks: 0 312 412 20 80
KEP Adresi : btk@btk.hs01.kep.tr

Bilgi için:. USOM
Birim Sorumlusu

IP/URL/ALAN ADI Listesi

Zaman Bilgisi	Domain/IP Adresi	Port	Protokol/Method
11.08.2025 21:18:36	46.197.5.147	445	tcp

TANIMLAR

Erişime Açık Dosya Paylaşımı Servisi: Erişime açık dosya paylaşımı servisi, söz konusu servislere ağ seviyesinde internet üzerinden tüm kullanıcıların erişebiliyor olması durumudur. İnternet üzerinden erişime açık dosya paylaşım servislerine yetkisiz erişim sağlanarak sistemin bütününü veya bir kısmını bozmaya yönelik girişimler olabilmektedir. Yapılan girişimlerin başarılı olması sonucunda, ilgili sistem ve/veya bağlı sistemlerde (istemciler, sunucular, mobil sistemler, vb.) siber güvenlik ihlali yaşanabilir. Siber güvenlik ihlallerine örnek olarak depolanan kritik veya gizli verilerin çıkarılması, sistem üzerinde istenmeyen değişiklikler yapılması, cihaz üzerindeki sistemlerin hizmet verememesi gösterilebilir.

Bu nedenle güvenlik sıkılaştırmaları yapılması, güncellemelerinin uygulanması, parola yönetimlerinin doğru şekilde yapılması ve erişim denetiminin gerçekleştirilmesi büyük önem arz etmektedir. İlgili servisin bilinen herhangi bir zafiyeti bulunmasa dahi sıfırıncı gün zafiyetlerinin de dikkate alınarak erişim kısıtlamalarının uygulanması gerekmektedir.

ALINMASI GEREKEN ÖNLEM VE EYLEMLER

1. KISA VADELİ ÖNLEM VE EYLEMLER (1-5 gün)

1.1. Söz konusu servislerin İnternet üzerinden erişimlerine ihtiyaç duyulmuyorsa erişimler kapatılmalıdır. Eğer ilgili servislerin internet üzerinden erişimine ihtiyaç var ise mümkünse yalnızca yetkilendirilmiş IP adreslerin erişimine izin verilecek şekilde kısıtlama uygulanmalıdır. Son kullanıcıların erişimleri kurumunmevcut ise süreli olarak VPN servisleri üzerinden yapılması sağlanmalıdır. İnternete açıkdosya paylaşım servislerine ait örnekler aşağıda paylaşılmaktadır.

AFP:548/tcp;FTP:21/tcp,2121/tcp;NFS:111/tcp;RSYNC:873/tcp;SMB: 445/tcp;TFTP:69/udp

1.2. İlgili servislere ve üzerinde çalışan işletim sistemlerine yönelik güvenlik güncellemeleri zaman kaybetmeksizin gerekli kontrollerden geçirilerek uygulanmalıdır.İnternete açık olması gereken servislerin güncellemelerine öncelik verilmelidir.

1.3. Hassas bilgilerin (kullanıcı adı, parola vb.) ağ üzerinde sadece güçlü algoritmalar kullanılarak şifrelenmiş (TLS vb.) bir şekilde iletildiğinden emin olunmalıdır. Şifrelenmemiş şekilde işlem yapan protokoller (ftp vb.) kullanılmamalıdır.

1.4. Güçlü parolalar seçilmelidir. Parolasız veya varsayılan kullanıcı adı/parola ile olan hesaplar kapatılmalıdır. Ayrıca parolalar; kurum adı, kişi adı, uygulama adı gibi bilgiler içermemelidir.

1.5. Misafir kullanıcı yetkilerine sahip kullanıcılar (Anonymous, Guest vb.) devre dışı bırakılmalıdır. Eğer kullanımına ihtiyaç var ise erişim yetkileri kontrol edilerek, hassas ve/veya gizli verilerin erişimlerine izin verilmemelidir.

1.6. Erişim denemelerinin gözlemlenebilmesi için gerekli iz kayıtlarının devrede olduğuna emin olunmalıdır.Ayrıca teknik imkanlar dahilinde hatalı erişim denemelerinde alarm mekanizmasının kurulması sağlanmalıdır.

1.7. İncelemeler sonrasında bu servisler üzerinden yetkisiz erişimlerin tespiti halinde adli bilişim incelemelerinin yapılması için ilgili kişiler/merciler ile iletişime geçilip hukuki süreç başlatılmalıdır.

2. ORTA VADELİ ÖNLEM VE EYLEMLER (1-4 hafta)

2.1. Olası yetkisiz erişim ile söz konusu sunucu/sunucular üzerinden ağda yayılma durumları gerçekleşebilir. Bu durumu tespit etmek için sunucular üzerindeki gerekli iz kayıtları ile birlikte kurum ağında bulunan diğer cihazların ve güvenlik duvarı gibi ağ cihazlarının iz kayıtları incelenmelidir. Olası anomalilerin tespiti için iz kayıt yönetimi araçlarından ve YARA kurallarından yararlanılabilir.

2.2. Tespit edilen zararlı aksiyonlarla, ilişkili sistem/uygulama belirtilerek USOM ile paylaşılmalıdır.

2.3. Servislerin ve/veya işletim sistemlerinin güvenlik yamaları takip edilmeli ve yama yönetimi iş süreci olarak tanımlanarak, güncel güvenlik yamaları zaman kaybetmeksizin gerekli kontrollerden geçirilerek uygulanmalıdır.

2.4. Yüksek yetki ile çalışan servis hesapları olası siber güvenlik ihlallerinde tüm sistemi tehlikeye atmaktadır. Söz konusu servis kullanıcılarının tam yetkili (root, administrator vb.) olmadığından emin olunmalıdır. Oluşturulan servis kullanıcısının dosya sistemi yetkileri kontrol edilerek iz kayıtlarına, yedeklere, yapılandırma dosyalarına ve kritik dosyalara erişimleri kısıtlanmalıdır.

2.5. İlgili sistemler üzerinde üretici firmaları ve USOM güvenlik bildirilerinde yayınlanan güncel zafiyetler takip edilmeli ve gerekli aksiyon ivedilikle uygulanmalıdır.

3. UZUN VADELİ ÖNLEM VE EYLEMLER

3.1. Sistemlerde gerçekleşebilecek veri hasarı/kaybı gibi durumlar için kritik verilerin (iz kayıt, yapılandırma, kritik dosyalar, vb) yedekleri düzenli olarak harici bir ortamda alınmalıdır.

3.2. Dosya paylaşım servislerinden hizmet alan kullanıcıların rolleri gözden geçirilmeli, erişim yetkileri kontrol edilerek yetkisiz erişimlerin olmadığından emin olunmalıdır.

3.3. Verilerin ve dosyaların kritiklik derecesi göz önünde bulundurarak, olası yetkisiz erişim durumlarına karşı dosya şifreleme araçlarından yararlanılmalıdır.

3.4. İnternetten erişime açık olması zorunlu olan servislerin kurum/kuruluş ağındaki diğer sunuculara kısıtlı erişimin olduğu bir ağiçinde olması sağlanmalıdır.

3.5. Teknik imkanlar dahilinde kritik servisler için ise iki faktörlü kimlik doğrulamanın devreye alınması sağlanmalıdır.

3.6. Gerekmediği sürece ilgili sunucuların İnternet yönünde olan trafikleri kapatılmalı veya kısıtlanmalıdır.

3.7. Kurumda siber olayların tekrar yaşanmaması için gerekli güvenlik önlemleri alınmalı ve

güvenlik sıkılaştırmaları yapılmalıdır.

3.8. Belirlenen tüm önlemlerin yeni kurulum yapılacak sistemlerde de uygulanabilmesi amacıyla, ilgili sistemler için kurulum prosedürü hazırlanması, erişim izinlerinin sıkılaştırılması, parola ve yama yönetimi konusuna yer verilmesi önerilmektedir.

NOT 1: Yukarıda belirtilen maddeler öneri mahiyetindedir. Bunların haricinde alınması gereken diğer bütün tedbirler kurumunuzun sorumluluğundadır.

NOT 2: Bildirimi yapılan IP Adreslerinin, kurumunuz yönetiminde bulunan Balküpü Sistemlerinin parçası olması durumunda herhangi bir aksiyon alınmasına gerek bulunmamaktadır. İlgili IP adresinin tarafımıza geri dönüş yapılması gerekmektedir.