KURUMLAR İÇİN SİBER GÜVENLİK ÖNLEMLERİNİ ÖLÇME TESTİ DOKÜMANI

Kurumlar İçin Siber Güvenlik Önlemlerini Ölçme Testi Dokümanı, kamu kurum ve kuruluşları ile özel sektör temsilcilerinin siber güvenlik adına almış olduğu önlemleri ve çalışmaları ölçmek amaçlı olarak hazırlanmıştır. Belirtilen sorulara verilen cevaplar ile Kurumunuzun siber güvenlik ve tehditler ile ilgili içinde bulunduğu durumu ayrıntılı olarak görme fırsatı doğacağı ve muhtemel siber güvenlik tehditlerine karşı daha etkili bir savunma sistemi kurulmasına neden olacağı değerlendirilmektedir. Ayrıca, bahse konu dokümanda yer alan sorulara karşılık gelen cevap veya cevapları herhangi bir kurum ile paylaşma zorunluluğu bulunmamaktadır.

Bu dokümanda yer alan 17 adet soruya verilecek cevaplar ile siber güvenliğin yönetişimi, siber güvenlik risklerinin ölçülmesi ve tanımlanması, bilgi sistemleri ve ağların korunması, ağlarda meydana gelebilecek kimliği ve nedeni tespit edilemeyen hareketlerin tespiti ve bazı siber güvenlik tehditleri ile ilgili tecrübeler hakkında ayrıntılı ve genel bir değerlendirme fırsatı elde edilmiş olunacaktır.

Son olarak, bahse konu dokümanın hazırlanmasında, "Framework for Improving Critical Infrastructure Cybersecurity", "Cybersecurity Examination Initiative" ve "Report on Cybersecurity Practices" adlı dokümanlardan faydalanılmıştır.

Siber Güvenlik Risklerinin Tanımlanması / Siber Güvenlik Yönetişimi

1. Aşağıda belirtilen ve kurumunuz tarafından bilgi güvenliği varlıklarının yönetimi amacıyla uygulanan her bir madde ile ilgili belirtilen işlemin;

- En son yapıldığı tarih,
- Gerçekleştirilme sıklığı,
- Gerçekleştirilmesinden sorumlu olan grup veya kişi,
- İşlemin kurum tarafından gerçekleştirilen kısımları (işlemin tamamı kurum tarafından gerçekleştirilmiyor ise)

bilgilerini göz önünde bulundurarak gerekli alanlara ait cevapları belirtiniz.

- Kurum içerisinde yer alan fiziksel cihazlar ve sistemler hakkında envanter tutulması.

- Kurum içerisinde yer alan yazılım platformları ve uygulamalar hakkında envanter tutulması.

- Ağ kaynakları, bağlantılar ve veri akışına ait haritalama ve ayrıntılı planlamanın oluşturulması veya güncellenmesi.

- Kurumun ağına bağlantılı dış kaynakların listelenmesi.

- Kaynakların (donanım, veri ve yazılım) önemine ve değerine göre korumak için önceliklendirilmesi.

- İz kaydı kapasitesinin ve uygulamalarının; yeterlilik, uygun saklama ve süreklilik kıstaslarını göz önünde bulundurarak belirlenmesi ve değerlendirilmesi.

2. Kurumunuza ait yazılı bilgi güvenliği politikasını belirtiniz.

3. Kurumunuz tarafından; siber güvenlik tehditlerini, açıklıklarını ve potansiyel sonuçlarını tespit etme adına periyodik olarak risk değerlendirilmesi yapılmakta mıdır? Eğer yapılıyorsa,

a. Kim tarafından yapılıyor ve hangi tarihte en güncel değerlendirme yapılmıştır?
b. En güncel risk değerlendirmenizden çıkan sonuçlar (hiçbir şey bulunamadı/ortalama/ yüksek risk) nelerdir?

4. Kurumunuz tarafından; siber güvenlik sorununa sebep olacak fiziksel siber güvenlik tehditlerini ve açıklıklarını tespit etme adına periyodik olarak risk değerlendirilmesi yapılmakta mıdır? Eğer yapılıyorsa,

a. Kim tarafından yapılıyor ve hangi tarihte en güncel değerlendirme yapıldı?
b. En güncel risk değerlendirmenizden çıkan sonuçlar (hiçbir şey bulunamadı/ortalama/ yüksek risk) nelerdir?

5. Kurumunuzda çalışanlar ve yöneticiler için siber güvenlik görevleri ve sorumlulukları açık ve detaylı olarak belirtilmiş ve atanmış ise, bunları detaylı olarak yazınız.

6. Herhangi bir siber güvenlik vakasının etkilerini azaltma ve/veya siber güvenlik vakasının ardından normal çalışma sürecine tekrar dönme adına kurumunuza ait yazılı iş sürekliliği sağlama dokümanını belirtiniz.

7. Kurumunuzda siber güvenlikten sorumlu ve yetkili bir yönetici (Chief Information Security Officer) veya eş değer bir pozisyon var mıdır? Eğer varsa, kişinin özellikleri ve sorumluluğu nedir? Eğer yok ise, kurumda muhtemel olabilecek bir siber güvenlik vakasında sorumlu/yetkili kim olacaktır?

8. Kurumunuza ait iş süreçlerine özgü en uygun siber güvenlik tedbirlerinin belirlenmesi nasıl yapılmaktadır?

9. Kurumunuzda, gerçekleşebilecek siber güvenlik vakasının ardından zararları ve harcamaları kapsayacak bir sigortalama mevcut mudur? Eğer mevcut ise, anılan bu sigortanın kapsamını ve içeriğini belirtiniz.

Kurumların Bilgi Sistemlerinin ve Ağlarının Korunması

10. Kurumunuz tarafından, bilgi güvenliği mimarisi ve süreçlerini modellemek için Türk Standartları Enstitüsü (TSE) veya Uluslararası Standartlar Örgütü (ISO) gibi kurumların yayımlamış olduğu *Siber Güvenlik Risk Yönetim Süreci* ile ilgili standartları konu alan dokümanlar kullanılmakta mıdır?

11. Aşağıda belirtilen her bir maddede, kurumunuz tarafından bilgi sistemlerinin ve ağlarının korunması için uygulanan politikaları ve prosedürleri yazılı olarak belirtiniz.

- Kurumunuz tarafından çalışanlarına, bilgi güvenliği riskleri ve sorumlulukları hakkında yazılı kılavuz ve/veya periyodik eğitim verilmekte midir? Cevabınız evet ise, anılan bu eğitimler ve/veya dokümanlar nelerdir ve en son hangi tarihte, hangi konularda düzenlenmiş ve kimlere verilmiştir?

- Kurumunuz tarafından, kuruma ait ağlarda meydana gelen veya meydana gelebilecek herhangi bir yetkisiz erişim teşebbüsü veya normal olmayan bir hareket tespiti adına kontrol araçları mevcut mudur? Cevabınız evet ise, anılan bu kontrolleri belirtiniz.

- Kurumunuz tarafından; işlerin sürekliliği ve ağlara zarar gelmemesi adına, kullanıcıların bu ağları kullanması kısıtlanmış mıdır? Cevabınız evet ise, hangi tür kontroller sebebi ile hangi kısıtlamalar yapılmıştır?

- Kurumunuz tarafından, kendi çalışma ortamından bağımsız bir biçimde işletilen ve kurumda kullanılan yazılımları ve uygulamaları test etmekte kullanılan başka bir ortam mevcut mudur? Cevabınız evet ise, detaylandırınız.

- Kurumunuz tarafından, benimsenen ve sürdürülen temel donanım ve yazılım yapılandırma ayarları bulunmakta mıdır? Cevabınız evet ise, kullanıcıların bu temel yapılandırma ayarlarını, yetkililerin izni ve onayı olmadan değiştirmeleri engellenmiş midir?

- Kurumunuzda, Bilgi Teknolojileri (Information Technologies – IT) varlıklarının sökülmesi, transfer edilmesi ve yerleştirilmesi adına oluşturulmuş bir süreç yönetimi planı mevcut mudur? Cevabınız evet ise, detaylandırınız.

- Kurumunuzda, güvenlik açıklarına karşılık gelen yazılım yamalarının periyodik olarak yüklenmesini de içeren, düzenli bir sistem bakım süreci mevcut mudur? Cevabınız evet ise, detaylandırınız.

- Kurumunuzun bilgi güvenliği politikalarında ve eğitimlerinde, taşınabilir ve mobil medya kullanımı hakkında bilgi var mıdır? Cevabınız evet ise, detaylandırınız.

- Kurumunuzun internete açılan IP adreslerine yönelik gerçekleşebilecek DDoS atağına karşı alınmış önlem var mıdır? Cevabınız evet ise, alınan koruma önlemlerinin neler olduğunu ve bu koruma önlemlerinden kimin sorumlu olduğunu belirtiniz?

- Kurumunuza ait yazılı bir veri imha politikası var mıdır? Cevabınız evet ise, detaylandırınız.

- Kurumunuza ait yazılı siber olaylara müdahale politikası mevcut mudur? Cevabınız evet ise, en son hangi tarihte güncellendiğini belirtiniz.

- Kurumunuza ait siber olaylara müdahale politikası düzenli olarak tatbikatlar ve testler ile değerlendirilmekte midir? Cevabınız evet ise, bu değerlendirmeler en son hangi tarihte ve kimin tarafından yapılmıştır?

- Kurumunuz tarafından, yedekleme sisteminin düzgün çalışıp çalışmadığı periyodik olarak test edilmekte midir? Cevabınız evet ise, en son hangi tarihte test edilmiştir?

12. Kurumunuz tarafından şifreleme kullanılmakta mıdır? Cevabınız evet ise, hangi kategorilerde ve şartlarda veri, iletişim ve cihazlar şifrelenmektedir?

13. Kurumunuz tarafından, düzenli olarak bilgi güvenliği politikalarının uygunluğu denetlenmekte midir? Cevabınız evet ise, en son denetleme ne zaman ve kimin tarafından gerçekleştirilmiştir?

14. Kurumunuza ait web sitesi veya ağlarına son bir yıl içinde DDoS (Distributed Denial of Service) atağına maruz kalmış mıdır? Cevabınız evet ise, saldırının süresi ve kurumunuza etkisini belirtiniz.

Kurum Ağlarında, Yetkisiz Erişim Eylemlerinin Tespit Edilmesi

15. Kurumunuz ağlarında meydana gelen veya gelebilecek yetkisiz erişim eylemlerini tespit etmek için aşağıda belirtilen maddelerin nasıl ve kim(ler) tarafından yerine getirildiğini belirtiniz.

- Yetkisiz erişim eylemlerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması,

- Kurum ağlarında gerçekleşmesi normal karşılanan olayların belirlenmesi,

- Farklı kaynaklar üzerinden elde edilen iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon),

- Önceden belirlenmiş siber olay alarmlarının ve bunlara karşılık gelen eşik değerlerinin belirlenmesi,

- Kurum ağlarının yaşanması muhtemel siber olaylara karşı sürekli olarak gözlemlenmesi,

- Kurum ağlarında çalışan muhtemel zararlı kodları tespit etmek için yazılım (Anti-Virüs vb.) kullanılması,

- Kurumun ağlarında bulunan yetkisiz kullanıcıların, cihazların, bağlantıların ve yazılımların izlenmesi,

- Veri kaybı engelleme yazılımlarının kullanılması,

- Kurum ağlarına yönelik sızma testlerinin ve zafiyet arama çalışmalarının gerçekleştirilmesi,

- Siber olay tespit süreçlerinin doğruluğunun gözden geçirilmesi,

- Kurumun siber güvenlik politikaları ve ölçütlerin geliştirilebilmesi için, siber olayların analiz edilmesi.

16. Kurum bilgisayarlarında ve/veya ağlarında, son bir yıl içinde tespit edilen zararlı yazılım(lar) oldu mu? Cevabınız evet ise, zararlı yazılım(lar)ın hangi hizmetleri etkilediğini, ne kadar süre kurum ağlarında çalıştığını, kurum ağlarına nasıl bulaştığını ve özelliklerini belirtiniz.

17. Kurum ağlarından, son bir yıl içerisinde yetkisiz kullanıcılar tarafından bilgi kaçırılmasına yönelik herhangi bir olay gerçekleşti mi? Cevabınız evet ise, yetkisiz kullanıcının kurum ağlarına nasıl sızdığını, kurum ağlarında ne kadar süre kaldığını, anılan saldırının sonuçlarını, kurumun bu saldırıyı nasıl öğrendiğini ve bu saldırıya karşı nasıl karşılık verildiğini belirtiniz.