[Gbl. Saltuk Buğra SOLMAZ (ORCİD: 0000-0001-9767-5247)

E-Posta: gblsolmaz@gmail.com C.Tlf:0506587 17 91]

SİBER GÜVENLİK TARİHİNDEKİ DÖNÜM NOKTALARI: TEHDİTLERİN EVRİMİ VE SAVUNMA STRATEJİLERİ

Özet: Bu makale, siber güvenlik tarihindeki önemli dönüm noktalarını ve bu dönemlerde yaşanan tehditlerin evrimini inceler. İlk olarak, bilgi teknolojilerinin yükselişiyle birlikte ortaya çıkan temel güvenlik zorlukları ele alınır. Ardından, siber saldırıların ve siber suç faaliyetlerinin hızla arttığı dönemler vurgulanır. Örnek olarak, 1980'lerdeki ilk bilgisayar solucanlarından 2000'lerdeki büyük ölçekli veri ihlallerine ve fidye yazılımlarının yükselişine kadar çeşitli önemli olaylar ve saldırılar üzerinde durulur. Bununla birlikte, makalede ayrıca bu dönemlerde geliştirilen savunma stratejileri ve siber güvenlik endüstrisinin nasıl evrildiği üzerinde durulur. Yeni tehditlere karşı güvenlik önlemlerinin nasıl geliştirildiği, siber güvenlik eğitiminin ve farkındalığın arttırılmasının önemi de ele alınır. Son olarak, makale, günümüzdeki siber güvenlik tehditlerinin karmaşıklığını ve gelecekteki eğilimleri tartışarak okuyucuları bilgilendirir.

Abstract: This article examines significant turning points in the history of cybersecurity and the evolution of threats during these periods. It first addresses the fundamental security challenges that emerged with the rise of information technologies. Subsequently, it highlights eras when cyber attacks and cybercrime activities rapidly increased. Examples include the first computer worms in the 1980s, large-scale data breaches in the 2000s, and the rise of ransomware. Additionally, the article focuses on the development of defense strategies and the evolution of the cybersecurity industry during these periods. It discusses how security measures have been developed against emerging threats and emphasizes the importance of cybersecurity education and awareness. Finally, the article informs readers by discussing the complexity of current cybersecurity threats and future trends.

Anahtar Kelimeler: Siber güvenlik tarihi, Tehditlerin evrimi,Dönüm noktaları, Bilgi teknolojisi güvenliği, Siber saldırılar, Siber suçlar, Bilgisayar solucanları, Veri ihlalleri, Fidye yazılımları,Savunma stratejileri, Siber güvenlik endüstrisi

Keys: Cybersecurity history, Threat evolution, Turning points, Information technology security, Cyber attacks, Cybercrime, Computer worms, Data breaches, Ransomware, Defense strategies, Cybersecurity industry

GİRİŞ

Siber güvenlik, bilgi teknolojileri ve dijital sistemlerin, bilgisayar ağlarının ve elektronik cihazların korunması ve güvende tutulması için alınan önlemlerin bütünüdür. Günümüzde hızla gelişen dijital dünyada, siber güvenlik önemi giderek artmaktadır. Siber saldırılar, veri ihlalleri ve siber suçlar gibi tehditler, bireyler, kurumlar ve devletler için ciddi riskler oluşturabilmektedir. Bu nedenle, siber güvenlik, bilgi güvenliği ve dijital varlıkların korunması için hayati bir öneme sahiptir.

[Gbl. Saltuk Buğra SOLMAZ (ORCİD: 0000-0001-9767-5247)

E-Posta: gblsolmaz@gmail.com C.Tlf:0506587 17 91]

Siber güvenlik tarihinde birçok önemli dönüm noktası yaşanmıştır. İlk olarak, bilgi teknolojilerinin yükselişiyle birlikte ortaya çıkan temel güvenlik zorlukları ele alınmalıdır. Bilgisayar ağlarının ve dijital sistemlerin yaygınlaşmasıyla birlikte, bilgi güvenliği tehditleri de artmıştır. Bilgisayar korsanları, kötü amaçlı yazılım geliştiricileri ve siber suçlular, hedeflerine yönelik saldırılarını geliştirmiş ve sofistike yöntemler kullanmaya başlamışlardır. Verilerin çalınması, kişisel bilgilerin ifşa edilmesi ve sistemlerin çökmesi gibi durumlar siber güvenliği tehdit eden başlıca sorunlardır.

Siber güvenlik tarihindeki önemli dönüm noktaları arasında ilk bilgisayar solucanlarından büyük ölçekli veri ihlallerine kadar çeşitli olaylar bulunmaktadır. 1980'lerdeki ilk bilgisayar solucanları, siber güvenlik açısından önemli bir dönüm noktası olarak kabul edilir. Bu solucanlar, bilgisayarlara bulaşarak kendini çoğaltabilen ve yayılan zararlı yazılımlardı. Bu saldırılar, bilgisayar ağlarının ve sistemlerin zayıf noktalarını ortaya çıkarmış ve güvenlik önlemlerinin geliştirilmesine yönelik bir uyarı niteliği taşımıştır.

2000'lerde ise büyük ölçekli veri ihlalleri ve fidye yazılımlarının yükselişi dikkat çekmiştir. Özellikle finansal kurumlar, şirketler ve hükümet kurumları hedef alınmış ve önemli miktarda veri çalınmış veya şifrelenmiştir. Bu tür saldırılar, siber güvenlik açısından büyük bir tehdit oluşturmuş ve savunma stratejilerinin geliştirilmesini zorunlu kılmıştır.

Bilgi teknolojilerinin hızla gelişmesi ve yaygınlaşmasıyla birlikte, siber güvenlik zorlukları da artmıştır. Cihazlar arasındaki bağlantılar, bulut bilişim, mobil uygulamalar ve nesnelerin interneti gibi yeni teknolojiler, daha fazla güvenlik riski oluşturmuştur. Siber suçlular, bu teknolojileri hedef alarak yeni saldırı yöntemleri geliştirmişlerdir.

Siber güvenlik, bilgi teknolojilerindeki gelişmelerin sunduğu fırsatlar ve beraberinde gelen siber suçlar ile mücadeleye ilişkin veri tabanlarının, bilgi sistemlerinin ve uygulamaların güvenliğinin sağlanmasının önemini artırmıştır (Öztürk, 2018: 209). Siber güvenliğe ilişkin yapılan en önemli düzenlemelerden biri 2015 yılında COSO ve Deloitte tarafından yayınlanan "COSO in the Cyber Age" raporudur. Bu rapor, siber riskin işletmedeki değerlendirilme süreçleri üzerine bir çerçeve sunmaktadır (COSO, 2015).

Sonuç olarak, siber güvenlik tarihi, bilgi teknolojilerinin yükselişiyle birlikte ortaya çıkan önemli dönüm noktalarını içermektedir. Siber saldırıların ve veri ihlallerinin artması, güvenlik zorluklarını da beraberinde getirmiştir. Bu nedenle, bilgi güvenliği ve siber güvenlik önlemlerinin sürekli olarak güncellenmesi ve iyileştirilmesi gerekmektedir. Gelecekteki eğilimlere ve tehditlere karşı hazırlıklı olmak için siber güvenlik bilincinin artırılması, savunma stratejilerinin geliştirilmesi ve işbirliği önem taşımaktadır."

Siber Risk Kavramına Genel Bakış

Günümüzde artan rekabet koşullarıyla birlikte, hem özel sektörde hem de kamu sektöründe bilgi teknolojileri yaygın şekilde kullanılmakta, işlemler elektronik ortamda gerçekleştirilmekte ve raporlama yapılmaktadır. Bilgi teknolojileri, birçok

[Gbl. Saltuk Buğra SOLMAZ (ORCİD: 0000-0001-9767-5247)

E-Posta: gblsolmaz@gmail.com C.Tlf:0506587 17 91]

kolaylık sağlamanın yanı sıra riskleri de beraberinde getirmektedir (Öztürk, 2018: 208). Siber risk kavramı da bu bağlamda önem kazanmaktadır.

Siber risk, bilgi teknolojileri ve dijital sistemlerin kullanımıyla ortaya çıkan tehditlerin ve olumsuz etkilerin bir sonucudur. Bu riskler, siber saldırılar, veri ihlalleri, kötü amaçlı yazılımlar ve diğer dijital tehditler şeklinde ortaya çıkabilir. Artan dijitalleşme ve bağlantılı cihazlar, kurumların ve bireylerin maruz kaldığı siber riskleri artırmaktadır.

Özellikle 12 Mayıs 2017 tarihinde gerçekleşen "WannaCry" adlı siber saldırı, siber riskin etkisini açıkça gösteren bir örnektir. Bu saldırı, ağırlıklı olarak Avrupa ülkelerini etkilemiş ve birçok kurumu ve kullanıcıyı hedef almıştır. "WannaCry" ransomware olarak adlandırılan bir fidye yazılımıydı ve birçok bilgisayarı etkileyerek dosyaları şifrelemiş ve fidye talep etmiştir. Bu saldırı, siber riskin gerçek bir tehdit olduğunu ve küresel çapta ciddi etkilere yol açabileceğini göstermiştir.

BadRabbit, 2017 yılında ortaya çıkan bir fidye yazılımı saldırısıdır. Bu saldırı, bilgisayar sistemlerine sızarak dosyaları şifreleyen ve ardından fidye talep eden bir saldırı türüdür. BadRabbit fidye yazılımı, özellikle Rusya, Ukrayna ve Türkiye gibi ülkelerde yaygın olarak etkili olmuştur.

Siber riskler, sadece siber saldırılardan ibaret değildir. Bilgi teknolojilerinin kullanımıyla birlikte veri ihlalleri, kötü amaçlı yazılımlar, phishing (kimlik avı), kimlik hırsızlığı gibi tehditler de ortaya çıkmaktadır. Örneğin, bir şirketin veya hükümet kurumunun verilerinin çalınması veya ifşa edilmesi, ciddi itibar kaybına ve maddi zararlara yol açabilir. Bu nedenle, siber risklerle mücadele etmek ve önlem almak önemlidir.

Siber risklerle başa çıkmak için kurumlar ve bireyler, etkili güvenlik önlemleri almalı ve siber güvenlik bilincini artırmalıdır. Bu, güçlü şifreler kullanmak, güvenlik yazılımları ve güncellemeleri düzenli olarak kullanmak, verileri yedeklemek ve güvenli internet kullanımı konusunda dikkatli olmak gibi tedbirleri içerir. Ayrıca, güvenlik açıklarını tespit etmek ve gidermek için düzenli olarak güvenlik testleri yapılmalıdır.

Siber risklerin artmasıyla birlikte, siber güvenlik alanında da sürekli gelişmeler ve yenilikler yaşanmaktadır. Yeni tehditler ortaya çıktıkça, savunma stratejileri ve teknolojileri de buna uygun olarak güncellenmektedir. Bu sürekli değişen ve gelişen ortamda, siber risklere karşı sürekli bir farkındalık ve hazırlıklı olmak önemlidir.

Bu bağlamda, bilgi teknolojilerinin yaygın kullanımıyla birlikte siber riskler de artmaktadır. Siber saldırılar, veri ihlalleri ve diğer tehditler, kurumlar ve bireyler için ciddi riskler oluşturmaktadır. Bu nedenle, siber risklere karşı tedbirler almak, güvenlik önlemlerini güncellemek ve siber güvenlik bilincini artırmak önem taşımaktadır. Yeni tehditlere karşı hazırlıklı olmak için siber risklerin sürekli olarak izlenmesi ve güncel gelişmelere uyum sağlanması gerekmektedir.

Siber Saldırılar Ve Doğal Afetler Sonrası Siber Güvenlik Sorunları

[Gbl. Saltuk Buğra SOLMAZ (ORCİD: 0000-0001-9767-5247)

E-Posta: gblsolmaz@gmail.com C.Tlf:0506587 17 91]

Geçmişte yaşanan siber saldırılar ve tanımsal ifadelerin ardından bilgi sistemlerine yönelik gerçekleştirilen yaygın siber tehditler aşağıdaki şekildedir (Kumar, Srivastava, & Lazarevic, 2005: 5-6):

Bilgisayar Solucanları: İlk bilgisayar solucanları, siber saldırı tarihinde önemli bir dönüm noktasıdır. Solucanlar, bilgisayarlara bulaşarak kendini otomatik olarak çoğaltabilen ve yayılan zararlı yazılımlardır. Örnek olarak, 1988 yılında Morris Solucanı (Morris Worm) bilgisayar ağlarında büyük çaplı hasara neden olmuştur.

Dosya ve Veri İhlalleri: Saldırganların hedef alarak yetkisiz erişim sağladığı veya çaldığı dosya ve veri ihlalleri siber saldırıların sık görülen bir türüdür. Bu saldırılarla birlikte, kişisel bilgilerin ifşa edilmesi, finansal verilerin çalınması veya ticari sırların ele geçirilmesi gibi ciddi sorunlar ortaya çıkabilir.

Kimlik Hırsızlığı: Siber saldırganlar, kişisel bilgileri ele geçirerek veya sahte web siteleri aracılığıyla kimlik hırsızlığı yapabilirler. Bu sayede, kullanıcıların banka hesaplarına veya diğer hassas bilgilere yetkisiz erişim sağlanabilir.

DDoS Saldırıları: Dağıtılmış Hizmet Reddi (DDoS) saldırıları, bir hedef sistem veya ağa aşırı miktarda trafik göndererek kaynakları tüketir ve sistemi hizmet dışı bırakır. Bu saldırılar, genellikle birçok kaynaktan eşzamanlı olarak gerçekleştirilir ve hedef sistem üzerinde aşırı yük oluşturur.

Fidye Yazılımları: Fidye yazılımları, kullanıcının dosyalarını şifreleyen ve dosyaların açılması için fidye talep eden zararlı yazılımlardır. Kullanıcılar genellikle dosyalarını geri alabilmek için fidye ödemek zorunda kalırlar.

Yukarıdaki sıralanan tehditlerin yanında Aslay (2017: 25-26) tarafından; sosyal mühendislik, web sayfası hırsızlığı ve yönlendirme, hukuka aykırı içerik sunulması, sistem güvenliliğinin kırılarak içeri sızılması, yerine geçme, çöpe dalma, istem dışı alınan elektronik postalar, bukalemun, oltalama, mantık bombaları, zararlı yazılımlar, bilgi ve veri aldatmacası, salam tekniği ve süper darbe gibi siber saldırı türleri sıralanmıştır.

Doğal afetlerin ardından ortaya çıkabilecek siber sorunlar da dikkate alınmalıdır. Örneğin, bir doğal afet sonrasında iletişim hatları veya altyapı sistemleri hasar görebilir ve bu da siber saldırılara açık hale gelebilir. Ayrıca, doğal afetler sırasında sahte yardım kuruluşları veya dolandırıcılık girişimleri gibi sosyal mühendislik saldırıları da artabilir.

Siber saldırılar ve doğal afetlerin birleşimi, ciddi sonuçlar doğurabilir. Özellikle acil durum yönetimi, kritik altyapıların korunması ve siber güvenlik tedbirlerinin alınması önem taşımaktadır. Bu tür olaylara karşı hazırlıklı olmak ve güvenlik önlemlerini güncel tutmak, ciddi zararların önlenmesine yardımcı olabilir.

Siber Saldırlarda Kişisel ve Kurumsal Savunma Mekanizmaları

Siber saldırılar, hem bireyleri hem de kurumları hedef alan ciddi tehditlerdir. Bu saldırılara karşı etkili savunma mekanizmaları oluşturmak, hem kişisel güvenliği korumak hem de kurumsal ağları güvende tutmak için hayati önem taşır. İşte siber saldırılara karşı kişisel ve kurumsal savunma mekanizmaları:

[Gbl. Saltuk Buğra SOLMAZ (ORCİD: 0000-0001-9767-5247)

E-Posta: gblsolmaz@gmail.com C.Tlf:0506587 17 91]

Kişisel Savunma Mekanizmaları:

- Güçlü Parolalar Kullanmak: Karmaşık ve benzersiz parolalar oluşturun. Parolalarınızı düzenli olarak değiştirin ve iki faktörlü kimlik doğrulama yöntemlerini kullanın.
- Bilinçli E-posta Kullanımı: Şüpheli veya tanımadığınız kişilerden gelen e-postalara karşı dikkatli olun. E-posta eklerini veya bağlantılarını açmadan önce güvenilirliklerini doğrulayın. Phishing e-postalarına karşı bilinçli olun ve kişisel bilgilerinizi paylaşmaktan kaçının.
- Güncel Yazılımları Kullanmak: İşletim sisteminizi ve uygulamalarınızı güncel tutun. Antivirüs ve antimalware yazılımlarını düzenli olarak güncelleyin.
- Bilinçli İnternet Kullanımı: Şüpheli web sitelerinden uzak durun ve güvenilir kaynaklardan indirme yapın. Sosyal medya ve çevrimiçi platformlarda dikkatli olun, kişisel bilgilerinizi sınırlayın.
- Eğitim ve Farkındalık: Sık sık siber güvenlik konularında eğitim alın. Sosyal mühendislik saldırılarına karşı bilinçli olun ve güvenlik önlemlerini uygulayın.

Kurumsal Savunma Mekanizmaları:

- Ağ Güvenliği: Güvenlik duvarı ve güvenli ağ yapılandırması kullanın. Veri trafiğini izleyen güvenlik sistemleri kurun ve anormal aktiviteleri tespit edin.
- Veri Yedeklemesi ve Kurtarma Planı: Önemli verilerin düzenli olarak yedeklenmesini sağlayın. Veri kaybı durumunda kurtarma planı ve süreklilik stratejileri oluşturun.
- Yetkilendirme ve Erişim Kontrolleri: Kullanıcıların yetkilendirme düzeylerini belirleyin ve gereksiz erişimleri kısıtlayın. Çok faktörlü kimlik doğrulama yöntemlerini uygulayın.
- Personel Eğitimi: Çalışanlara siber güvenlik politikaları ve en iyi uygulamalar hakkında eğitim verin. Sosyal mühendislik saldırılarına karşı farkındalığı artırın.
- Sürekli İzleme ve Güncelleme: Sistemlerinizi ve yazılımlarınızı düzenli olarak güncelleyin. Ağ trafiğini izleyerek anormal aktiviteleri tespit edin ve hızlı müdahale yapın.

Bu savunma mekanizmalarının etkin bir şekilde uygulanması, siber saldırılara karşı direnci artırır ve kişisel bilgilerin ve kurumsal verilerin güvende kalmasını sağlar. Herkesin siber güvenlik konusunda bilinçli olması ve güvenlik önlemlerini almaya özen göstermesi önemlidir.

Genel Olarak Siber Saldırılara Karşı Önlemler

I. Güçlü Parolalar Kullanın:

- Karmaşık ve benzersiz parolalar oluşturun.
- Parolalarınızı düzenli olarak değiştirin.
- İki faktörlü kimlik doğrulama yöntemlerini kullanın.

II. Güncel Yazılımları Kullanın:

[Gbl. Saltuk Buğra SOLMAZ (ORCİD: 0000-0001-9767-5247)

E-Posta: gblsolmaz@gmail.com C.Tlf:0506587 17 91]

- İşletim sistemlerini, uygulamaları ve antivirüs yazılımlarını güncel tutun.
- Yazılımlarınızın otomatik güncelleme özelliğini etkinleştirin.

III. E-posta Güvenliği:

- Şüpheli veya tanımadığınız kişilerden gelen e-postalara karşı dikkatli olun.
- E-posta eklerini veya bağlantılarını açmadan önce güvenilirliklerini doğrulayın.
- Phishing e-postalarına karşı bilinçli olun ve kişisel bilgilerinizi paylaşmaktan kaçının.

IV. Veri Yedeklemesi:

- Önemli verilerinizi düzenli olarak yedekleyin.
- Yedeklemeleri güvenli bir ortamda saklayın ve doğrulama yapın.
- Veri kaybı durumunda yedeklemeleri kullanarak verilerinizi kurtarabilirsiniz.

V. Ağ Güvenliği:

- Güvenlik duvarı ve güvenli ağ yapılandırması kullanın.
- Wi-Fi ağınızı şifreleyin ve varsayılan yönetici şifrelerini değiştirin.
- Ağ trafiğini izlemek ve zararlı etkinlikleri tespit etmek için güvenlik sistemleri kullanın.

VI. Personel Eğitimi:

- Çalışanlarınıza güvenli internet kullanımı, e-posta güvenliği ve şüpheli içerikleri tanıma konularında eğitim verin.
- Sosyal mühendislik saldırılarına karşı bilinçlendirme yapın ve güvenlik politikalarını belirleyin.

VII. Kriz Planı ve İzleme:

- Bir siber saldırı durumunda kriz planınızı hazır tutun.
- Güvenlik olaylarını izlemek ve anormal aktiviteleri tespit etmek için güvenlik olay yönetimi sistemleri kullanın.

VIII. Harici Cihazlara Dikkat:

- USB bellek, harici hard disk gibi cihazları dikkatli bir şekilde kullanın.
- Bilinmeyen kaynaklardan gelen cihazları takmadan önce güvenilirliğini doğrulayın.

IX. Uzman Yardımı ve İzleme:

- Bir siber güvenlik uzmanından yardım alın ve sistemlerinizi düzenli olarak denetletin.
- Güvenlik güncellemelerini ve tehditleri takip etmek için güvenlik duvarı ve antivirüs yazılımlarını kullanın.

X. Farkındalık ve Sürekli Öğrenme:

[Gbl. Saltuk Buğra SOLMAZ (ORCİD: 0000-0001-9767-5247)

E-Posta: gblsolmaz@gmail.com C.Tlf:0506587 17 91]

- Siber güvenlik konusunda kendinizi sürekli olarak güncelleyin.
- Yeni saldırı yöntemlerini, güvenlik önlemlerini ve en iyi uygulamaları takip edin.

Siber saldırılara karşı alınacak önlemler, bilgi güvenliği ve siber güvenlik politikalarının bir parçası olmalıdır. Sürekli olarak tehditleri değerlendirmek, güvenlik açıklarını tespit etmek ve önlemek için aktif bir yaklaşım benimsemek önemlidir. Güvenlik bilincini artırmak ve çalışanların eğitimine önem vermek, kurumunuzun siber saldırılara karşı daha dirençli olmasına yardımcı olacaktır.

Sonuç ve Değerlendirme

Siber güvenlik tarihindeki dönüm noktaları, tehditlerin evrimi ve savunma stratejilerinin gelişimi açısından önemli bir rol oynamıştır. Bu dönüm noktaları, bize siber güvenlik konusunda önemli dersler vermektedir.

Sürekli Bir Yarış:

Siber saldırganlar ve savunma uzmanları arasında sürekli bir yarış söz konusudur. Teknolojik gelişmeler ve yeni saldırı yöntemleri ortaya çıktıkça, savunma stratejileri de buna uyum sağlamak zorundadır. Bu yarış, siber güvenlik alanındaki önlemlerin sürekli olarak güncellenmesi ve iyileştirilmesi gerektiğini göstermektedir.

İşbirliği ve Paylaşımın Önemi:

Siber güvenlik tehditleri sınırları aşabilen bir niteliğe sahiptir. Bu nedenle, siber güvenlik açısından işbirliği ve bilgi paylaşımı büyük bir öneme sahiptir. Kurumlar, hükümetler, akademik kuruluşlar ve sivil toplum kuruluşları arasında işbirliği ve ortak çalışmalar, tehditlerle mücadelede daha etkili olmayı sağlayabilir.

Farkındalık ve Eğitimin Önemi:

İnsan faktörü, siber güvenlik açısından en önemli unsurlardan biridir. Kullanıcıların farkındalığı ve eğitimi, siber saldırılara karşı savunmanın temel bir unsuru olarak değerlendirilmelidir. Kullanıcıların güvenlik politikalarına uyması, güçlü şifreler kullanması, kimlik avı saldırılarını tanıması ve güvenlik açıklarına dikkat etmesi, kurumsal ve kişisel siber güvenliği artırmada büyük bir öneme sahiptir.

Sürekli İyileştirme ve İzleme:

Siber güvenlik, statik bir konu değildir. Tehditler sürekli olarak evrim geçirirken, savunma stratejileri de sürekli olarak iyileştirilmeli ve güncellenmelidir. Güvenlik açıklarının izlenmesi, zayıf noktaların tespit edilmesi ve düzeltilmesi süreci sürekli olarak devam etmelidir.

Sonuç olarak, siber güvenlik tarihindeki dönüm noktaları, tehditlerin karmaşıklığını ve çeşitliliğini ortaya koymuştur. Bu dönüm noktalarından çıkarılan dersler, siber güvenlik stratejilerinin sürekli olarak güncellenmesi, işbirliği ve paylaşımın teşvik edilmesi, farkındalık ve eğitimin öneminin vurgulanması ve sürekli iyileştirme ve izleme süreçlerinin uygulanması gerektiğini göstermektedir. Böylece, siber güvenlik açısından daha güçlü bir savunma mekanizması oluşturulabilir ve tehditlere karşı daha etkili bir şekilde mücadele edilebilir.

[Gbl. Saltuk Buğra SOLMAZ (ORCİD: 0000-0001-9767-5247)

E-Posta: gblsolmaz@gmail.com C.Tlf:0506587 17 91]

Kaynakça

American Accounting Association. (2017). Cybersecurity and Continuous Assurance. Journal Of Emergıng Technologıes In Accountıng , 1-12.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. International Journal of Multidisciplinary Studies and Innovative Technologies , 24- 28.

Burca, N. (2017, Haziran 3). İç Kontrolleriniz Etkin Mi? «WannaCry» Siber Saldırısında Sorumluluk Kime Ait? Mart 5, 2019 tarihinde https://nazifburca.com adresinden alındı

COSO. (2015). COSO in the Cyber Age: Report Offers Guidance on Using Frameworks to Assess Cyber Risks

İnternet Kaynakları

https://www.kaspersky.com.tr/blog/bad-rabbit-ransomware/4326/