TR Cybersecurity Alliance Faaliyetlerine Başladı

2023'ün son çeyreğinde Türkiye'nin önde gelen siber güvenlik profesyonelleri güçlerini birleştirerek TR Cybersecurity Alliance adında bir siber güvenlik ittifakı kurdu. İlk toplantısını Radisson Blu Ataşehir otelinde yapan ittifak, Türkiye'nin siber dayanıklılığını arttırmaya destek olacak çalışmalar yapmayı hedefliyor.

TR Cybersecurity Alliance Nedir?

TR Cybersecurity Alliance, Türkiye'nin çeşitli sektörlerinde görev yapmakta olan ve ortalama 15 yıldan fazla siber güvenlik deneyimi olan tanınmış sektör profesyonellerinin girişimi ile kurulan bir çalıştay grubudur. İttifak hakkında detaylı bilgi web sitesi ve LinkedIn sayfasında bulunmaktadır.

Neden Kuruldu?

TR Cybersecurity Alliance, Türkiye'nin siber güvenlik alanındaki zorlukları ele almak, bilgi paylaşımını teşvik etmek ve sektördeki en iyi uygulamaları benimsemek ve kaynak olarak sunmak amacıyla kuruldu. İttifak, siber tehditlere karşı etkin bir mücadele için birlikte çalışarak, topluluk içinde bilgi ve deneyim paylaşımını artırmayı amaçlamaktadır.

İttifakın Amacı Nedir?

Siber güvenlik teknik olarak son derece zor ve karmaşık bir alandır. Bu nedenle sayısız kanun, yönetmelik, regülasyon, standart veya kılavuz siber dayanıklılığı arttırmak için ilgili kurumlarca yayınlanmıştır. Siber güvenlik günümüzde ticari ve sosyal hayatın sürekliliği bakımından önemli olduğu kadar ulusal güvenlik açısından da büyük önem arz etmektedir. Kurum ve kuruluşlar bunca karmaşanın içinde hangi alanlara hangi sırayla nasıl yatırım yapacaklarını belirlemekte zorlanmakta ve yapılan yatırımların verimini ölçmekte güçlük yaşamaktadır.

TR Cybersecurity Alliance, Türkiye'nin önde gelen tanınmış siber güvenlik uzmanlarının deneyimlerini birleştirmek ve büyüyen deneyim havuzunu siber güvenlik stratejisi üretmekte zorlanan kurum ve kuruluşlara ücretsiz sunmak için kurulmuştur.

TR Cybersecurity Alliance'ın temel amaçları şunlardır:
- Türkiye'nin siber güvenlik altyapısını güçlendirmek için katkıda bulunmak
- İnovasyon ve araştırmayı teşvik ederek sektördeki en son gelişmelere ayak uydurmak
- Sektördeki profesyoneller arasında etkili iletişimi ve iş birliğini artırmak
- Kamu ve özel sektörde siber güvenlik konusundaki farkındalığı artırmak

Kimlerden Oluşur?

TR Cybersecurity Alliance, Türkiye'deki önemli finans, enerji, sigorta, e-ticaret kuruluşlarının IT guruları ve siber güvenlik alanındaki önemli üreticilerin uzmanlarını bir araya getirir. İttifak, üyelerinin çeşitli uzmanlık alanlarından gelmesini ve birbirleriyle etkileşimde bulunarak güçlü bir bilgi havuzu oluşturmayı amaçlar.

Çalışma Düzeni Nedir?

TR Cybersecurity Alliance en geç her çeyrek düzenli olarak toplantılar ve çalıştaylar düzenleyerek üyeleri arasında etkileşimi artırır. Bu etkinliklerin amacı ittifak üyelerinin deneyimlerini birleştirmek ve her kurum veya şirketin uygulayabileceği çözüm önerileri üretmektir. Siber güvenlik disiplinleri veya regülasyonları da ittifakın çalışma alanlarına girmektedir. Bu anlamda ittifak yönetici veya düzenleyici kamu kurumlarına da öneriler üretmek için özel çalışmalar yapacaktır.

TR Cybersecurity Alliance ile Bağlantı Kurun

Web Sitesi: www.tr-csa.org
LinkedIn: TR Cybersecurity Alliance - www.linkedin.com/company/tr-cybersecurity-alliance

Kimlerden Oluşur?

TR Cybersecurity Alliance, Türkiye'deki önemli finans, kamu, enerji, telekom, lojistik, sigorta ve e-ticaret gibi kurum ve kuruluşlarının siber güvenlik uzmanlarının katılımı ile kurulmuştur. Ayrıca Nebula, Binalyze, Picus, SecHard ve Trellix gibi yerli ve yabancı önemli siber güvenlik firmaları tarafından desteklenmektedir.

TR CYBERSECURITY ALLIANCE

Üyeler


Ahmet Özkan


Ahmet Öztoprak


Akın Börekçi


Ali Tursun


Alper Şulan


Alvaro Garcia


Ayed Al Qartah


Caner Dağlı


Cem Dursun


Cengiz Keskin


Cihan Yücer


Deniz Şener


Erhan Güleyüpoğlu


Ferhat Arpacı


Gürsel Arıcı


İlker Çağrı Güven


Kayıhan Altınoz


Metin Eser


Murat Zaralı


Nedim Kaya


Nusret Karakaya


Ömer Çuhadaroğlu


Özgür Orhan


Savaş Ergen


Serkan Akcan


Serkan Kırmızıgül


Tonyukuk Özden


Tuncay Arslan


Yusuf Usta

TR CYBERSECURITY ALLIANCE

Malware (Kötücül Yazılım) Korumasında En İyi 10 Uygulama

GİRİŞ

Türkiye'nin önde gelen siber güvenlik uzmanları tarafından kurulan TR Cybersecurity Alliance, üyeleri ile birlikte siber güvenlik alanındaki en iyi uygulamaları belirleyerek, şirketlerin ve kamu kurumlarının siber güvenliklerini güçlendirmeyi amaçlamaktadır. Çalıştay sonucunda ortaya çıkan bu En İyi Uygulamalar (Best Practice) dokümanı, malware korumasıyla ilgili temel prensipleri içermekte olup, kurumların siber dayanıklılığını artırmasına rehberlik etmek amacıyla tasarlanmıştır.

Malware (Kötücül Yazılım) Korumasında En İyi 10 Uygulama

1. Varlık Yönetimi

Siber güvenliğin her alanında atılması gereken ilk adım dijital varlıkların yönetilmesidir. Keşif özelliği bulunan varlık yönetim araçları ile bilişim sisteminde bulunan veya gelecek zamanlarda sisteme eklenecek olan tüm varlıklar tespit edilmeli, gerekli güvenlik denetimi ve uygulamaları tercihen otomatik olarak yapılmalıdır.

2. Kullanıcı Eğitimi ve Simülasyonu

Tüm BT varlıklarının muhatapları kullanıcılarıdır ve siber güvenlik ancak kullanıcıların bilinç seviyesi kadar güçlü olabilir. Her türlü regülasyon ve standardın ötesinde, kullanıcılara geniş içerikli ve oldukça sık eğitimler verilmeli, oltalama simülatörü gibi araçlarla bilinç düzeyleri sınanmalıdır.

3. Endpoint Protection Platform (EPP) ve Endpoint Detection and Response (EDR) Kullanımı

Günümüzün siber güvenlik gerçekleri karşısında tüm kuruluşlar Endpoint Protection Platform (EPP) ve Endpoint Detection and Response (EDR) çözümlerini kullanmalıdırlar. Bu teknolojiler kötü amaçlı yazılımları tespit etme ve engellemede etkili yöntemlerdir. Tercih edilen ürünlerin teknik özelliklerine göre servislerin doğru çalışıp çalışmadığı önceden belirlenen bir program veya yöntem ile sürekli olarak sınanmalıdır.

4. Sandbox Çözümleri

Advanced Persistent Threat (APT) ataklarına karşı e-posta, dosya ve ağ gibi farklı vektörlerde çalışabilen Sandbox çözümleri konumlandırılmadır. Bu, çeşitli saldırı yöntemlerine karşı daha etkili bir koruma sağlar. Content Disarm & Reconstruction (CDR) araçları ise veri hijyenini sağlamak için önemli yardımlarda bulunur ve sıfır gün koruma kabiliyetini artırır.

5. Güvenlik Sıkılaştırmaları

Center for Internet Security (CIS) Windows 10 Benchmark analizlerine göre güvenlik sıkılaştırması uygulamak, başka bir güvenlik aracına gerek kalmadan zararlı yazılımları ortalama %70 oranında engellemeye olanak sağlar. Kurum ve kuruluşlar CIS Benchmark standartlarına uygun güvenlik sıkılaştırmalarını uygulamalı ve sürekli olarak güncellemelidir. Otoritelerce desteklenmeyen teknolojiler için özelleştirilmiş sıkılaştırma şablonları üretilmeli ve uygulanmalıdır.

6. Application Control Yazılımları

Application Control yazılımları, yalnızca belirlenmiş uygulamaların çalışmasına izin vererek, bilgisayar sistemlerinin güvenliğini artırır. Bu nedenle kurum ve kuruluşlar bu tür yazılımları etkili bir şekilde kullanmalıdır.

7. Table Top Exercises (Masa Üstü Egzersizleri)

Kurumlar, siber saldırı senaryolarını simüle eden masaüstü egzersizlerini risk seviyesine uygun bir frekansta ve yılda iki defadan az olmamak üzere gerçekleştirmelidirler.

8. Malware Saldırı Simülasyonları

Breach and Attack Simulation (BAS) araçları kullanılarak siber güvenlik sisteminin sağlıklı çalışıp çalışmadığı rutin aralıklarla test edilmelidir. Risk seviyesine göre belirlenmesi gereken aralıklar haftada bir veya yılda en az dört kez aralığında olmalıdır.

9. Olay Yanıtlama ve Adli Bilişim Planlaması

Siber saldırıları tamamen engellemek mümkün olmadığından kurumlar Olay Yanıtlama Planlarını oluşturmak zorundadırlar. Olay müdahale ekipleri şüpheli aktiviteleri hızlı bir şekilde tespit etmeli, düzeltici ve önleyici faaliyetlere başlayabilmelidir. Dijital deliller hızlı ve hassas bir şekilde toplandıktan sonra araştırma ve analiz yapılmalıdır. Tüm bu süreç tamamlandıktan ve tehditler değerlendirildikten sonra ortaya çıkan rapor ışığında iyileştirme eylemleri zamanında gerçekleştirilmelidir.

10. Siber Güvenlik Eğitimleri

Siber güvenlik ekipleri, yeni ortaya çıkan tehditleri, en son saldırı vektörlerini ve güvenlik teknolojilerindeki gelişmeleri kapsayan düzenli eğitim programlarına katılmalıdır. Pratik uzmanlığını arttırmak için uygulamalı eğitim oturumları ve atölye çalışmaları yapmalıdır. Beceriyi arttırmak ve genişletmek için sektörde kabul gören sertifikalara sahip olmak da önemlidir.

Çalıştay Sırasında Kullanılan Kaynak ve Regülasyonlar

- Center for Internet Security (CIS) Benchmarks
www.cisecurity.org/cis-benchmarks
- T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi – Bilgi ve İletişim Güvenliği Rehberi
www.cbddo.gov.tr/bigrehber/
- MITRE Attack Framework
www.attack.mitre.org/
- CISA (Cybersecurity & Infrastructure Security Agency)
www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Dokümanda Kullanılan Terimler Sözlüğü

Advanced Persistent Threat (APT – Gelişmiş Kalıcı Tehdit): Saldırganların bir ağa yetkisiz erişim sağlamak, kalıcılığı sürdürmek ve genellikle casusluk veya veri amacıyla hassas bilgileri uzun bir süre boyunca sızdırmak için hedefli ve gizli teknikler kullandığı karmaşık ve uzun süreli bir siber saldırıdır.

Application Control / Whitelisting (Uygulama Kontrolü): Uygulamaların uç noktalarda yürütülmesini düzenleyen ve izleyen, yalnızca yetkili programların çalışmasına izin veren ve yetkisiz veya kötü amaçlı programları önleyen, böylece saldırı yüzeyini ve potansiyel riskleri en aza indirerek genel güvenliği artıran bir siber güvenlik önlemidir.

Asset Management (Varlık Yönetimi): Doğru bir envanter sağlamak, güvenlik açıklarını değerlendirmek ve potansiyel tehditlere ve ihlallere karşı koruma sağlamak için etkili güvenlik önlemleri uygulamak amacıyla bir kuruluşun donanım, yazılım ve ağ varlıklarının sistematik olarak tanımlanması ve sürekli olarak izlenmesidir.

Breach and Attack Simulation (BAS – İhlal ve Saldırı Simülasyonu): Güvenlik kontrollerinin etkinliğini değerlendirmek ve doğrulamak, güvenlik açıklarını belirlemek, olaylara müdahale yeteneklerini geliştirmek ve sonuçta kuruluşun genel dayanıklılığını artırmak için bir kuruluşun sistemlerine gerçek dünyadaki siber saldırıların simüle edilmesini içeren proaktif bir siber güvenlik tekniğidir.

Center for Internet Security (CIS): Bilgi teknolojisi alanında en iyi güvenlik uygulamalarını teşvik eden, bu doğrultuda standartlar geliştiren, siber güvenliği artırmaya odaklanan ve kar amacı gütmeyen bir kuruluştur.

CIS Benchmark: Center for Internet Security (CIS) tarafından oluşturulan bir dizi güvenlik standartları ve önerileridir. Bu kılavuzlar, bilgisayar sistemlerinin ve ağların güvenliğini artırmak için endüstri standartlarını ve en iyi uygulamaları belirler.

Compromise Assessment (Tehdit Değerlendirmesi): Olası tehditleri analiz etmek ve proaktif olay müdahalesi için genel tehdit görünürlüğünü artırmak amacıyla gelişmiş tespit teknikleri ve araçlarından yararlanarak, bir güvenlik ihlali veya ihlaline ilişkin herhangi bir işareti tespit etmek ve değerlendirmek amacıyla bir kuruluşun ağını, sistemlerini ve uç noktalarını sistematik olarak değerlendiren bir siber güvenlik uygulamasıdır.

Content Disarm & Reconstruction (CDR - İçeriğin Silahsızlandırılması ve Yeniden İnşası): Dosyaları parçalara ayıran ve yeniden yapılandıran, temel içeriği korurken potansiyel kötü amaçlı öğeleri ortadan kaldıran, böylece e-posta ekleri veya diğer dosya aktarımları yoluyla kötü amaçlı yazılım bulaşma riskini azaltan bir siber güvenlik teknolojisidir.

Endpoint Detection and Response (EDR – Uç Nokta Tehdit Tespit ve Yanıtı): Bir kuruluşun ağındaki gelişmiş tehditleri, şüpheli davranışları ve güvenlik olaylarını belirlemek ve azaltmak için hızlı algılama, araştırma ve yanıt yetenekleri sağlayan, uç nokta etkinliklerini gerçek zamanlı olarak izleyen ve analiz eden bir siber güvenlik teknolojisidir.

Endpoint Protection Platform (EPP – Uç Nokta Koruma Yazılımı/Platformu): Gelişmiş algılama ve önleme mekanizmaları kullanarak, sunucular veya uç noktaları kötü amaçlı yazılım, fidye yazılımı ve yetkisiz erişim dahil olmak üzere çeşitli siber tehditlerden korumak için tasarlanmış kapsamlı bir güvenlik çözümüdür.**Forensic Planning (Adli Bilişim Planlaması):** Güvenlik olaylarını veya siber suçları araştırmak ve anlamak için dijital kanıtların sistematik bir şekilde toplanması, analiz edilmesi ve korunması için kapsamlı bir strateji geliştirmeyi, bilgilerin yasal ve soruşturma amaçlı olarak bütünlüğünü ve kabul edilebilirliğini sağlamayı içerir.

Incident Response Plan (Olay Yanıtlama Planı): Bir kuruluşun bir siber güvenlik olayı durumunda atması gereken adımları özetleyen, güvenlik ihlallerini veya siber saldırıları tespit etmek, müdahale etmek, hafifletmek ve kurtarmak için sistematik ve koordineli bir yaklaşım sağlayan, yapılandırılmış bir yazılı prosedürler dizisidir.

Malware (Kötücül Yazılım): Malware, bilgisayar sistemlerine veya kullanıcıların verilerine zarar vermek, izinsiz erişim sağlamak veya bilgi çalmak amacıyla tasarlanmış kötü niyetli yazılım türlerini ifade eder.

Phising (Oltalama): Saldırganların yanıltıcı e-postalar, mesajlar veya web siteleri kullanarak bireyleri kullanıcı adları, şifreler veya finansal ayrıntılar gibi hassas bilgileri ifşa etmeleri için kandırdıkları ve genellikle güvenilir kuruluşlar gibi davranarak kişisel veya kurumsal kimliklerini kötüye kullandıkları veya tehlikeye attıkları bir siber saldırı tekniğidir.

Sandbox (Kum Havuzu): Güvenilmeyen veya potansiyel olarak kötü amaçlı yazılımların güvenli bir şekilde yürütülüp analiz edilebildiği, siber güvenlik profesyonellerinin gerçek sisteme veya ağa zarar verme riski olmadan bu yazılımların davranışlarını değerlendirmesine olanak tanıyan güvenli ve yalıtılmış bir ortamdır.

Security Hardening (Güvenlik Sıkılaştırma): Bir sistemin veya ağ cihazının savunmasını güçlendirmek, güvenlik açıklarını en aza indirmek ve siber saldırı veya yetkisiz erişim potansiyelini azaltmak için güvenlik önlemlerinin, yapılandırmalarının ve en iyi uygulamaların sistematik olarak uygulanmasıdır.

Tabletop (Masaüstü) Egzersizleri: Bir organizasyonun kriz yönetimi veya siber güvenlik planlarını uygulama ve test etme amacıyla gerçek bir olayın simülasyonunu masa başında yapma egzersizidir.

SONUÇ

Organizasyonlar bu En İyi Uygulamalar (Best Practice) dokümanındaki önerilere uyarak siber dayanıklılıklarını artırabilir ve malware tehditlerine karşı daha etkili bir savunma sağlayabilirler. Siber güvenlik sürecinin devamlılık gerektirdiği unutulmamalıdır. Belirtilen prensiplere uyum sağlamak siber güvenlik seviyelerini artırarak organizasyonların daha güvenli bir çevrede faaliyet göstermelerine katkı sağlayacaktır.

Çalışmaya Katkıda Bulunanlar

Ahmet Özkan
Ahmet Öztoprak
Ali Tursun
Alvaro Garcia
Ayed Al Qartah
Caner Dağlı
Cihan Yüceer
Çağrı Güven
Ferhat Arpacı
Gürsel Arıcı
Kayıhan Altınöz
Metin Eser
Nedim Kaya
Ömer Çuhadaroğlu
Özgür Orhan
Serkan Akcan
Serkan Kırmızıgül
Tuncay Aslan
Yusuf Usta