TR CYBERSECURITY ALLIANCE

28 Şubat 2024

Ulusal Siber Güvenlik İçin İyileştirme Önerileri

TR Cybersecurity Alliance Nedir?

2023'ün son çeyreğinde Türkiye'nin önde gelen siber güvenlik profesyonelleri güçlerini birleştirerek TR Cybersecurity Alliance adında bir siber güvenlik ittifakı kurdu.

TR Cybersecurity Alliance, Türkiye'nin çeşitli sektörlerinde görev yapmakta olan ve ortalama on beş yıldan fazla siber güvenlik deneyimi olan tanınmış sektör profesyonellerinin girişimi ile kurulan bir çalıştay grubudur. Son iki çeyrekte çalışma grubunu devam ettiren TR Cybersecurity Alliance, Türkiye'nin siber dayanıklılığını arttırmaya destek olacak çalışmalar yapmayı hedefliyor. İttifak hakkında detaylı bilgi web sitesi ve linkedIn sayfasında bulunmaktadır.

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:

- 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

Çalışma Düzeni Nedir?

TR Cybersecurity Alliance her çeyrek düzenli olarak toplantılar ve çalıştaylar düzenleyerek üyeleri arasında etkileşimi artırır. Bu çalıştayların 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

Ulusal Siber Güvenlik İçin İyileştirme Önerileri

TR Cybersecurity Alliance üyeleri kamu hizmetlerinin güvenliği ve sürekliliği için aşağıdaki önerileri üretmiş ve tüm tarafların bilgisine sunmaya karar vermiştir.

1. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayınlanan Bilgi ve İletişim Güvenliği Rehberi'nin beş numaralı maddesi olan sıkılaştırma tedbirleri, güvenli konfigürasyonlara sahip olmak için önemli öneriler getirmiş olsa da teknik olarak yetersiz olduğu değerlendirilmektedir. Ağırlıklı olarak Linux ve Windows işletim sistemleri için düşünülmüş olan sıkılaştırma tedbirlerinin sayısı Center for Internet Security (CIS) Benchmark belgeleri ile karşılaştırıldığında eksik ve yetersiz kalmaktadır. Ayrıca Genel Sıkılaştırma Tedbirleri başlığı altında çeşitli öneriler bulunsa da ağ cihazları, veri tabanları web sunucular, sanallaştırma sistemleri, e-posta sunucuları ve internet tarayıcıları gibi birçok ürün ve uygulamada yeterli sıkılaştırma sağlandığı söylenemez. CIS kurumu tarafından yapılan araştırma (Kaynak 1) siber güvenlikte sıkılaştırma tedbirlerinin önemini ortaya koymaktadır. Güvenlik sıkılaştırma tedbirinin derinleştirilmesini ve tüm bilişim sistemlerini kapsayacak şekilde düzenlenmesini öneriyoruz.

2. Endpoint Detection and Response (EDR) ürün grubu siber güvenlik alanında kritik öneme sahiptir. Bu nedenle Amerika Birleşik Devletleri Başkanlık Yönetim Ofisi tarafından yayınlanan M-22-01 (Kaynak 2) numaralı muhtıra ile 8 Ekim 2021 tarihinde Amerikan devlet kurumlarına zorunlu hale gelmiştir. Gelişen teknoloji ile EDR ürünleri evrim geçirerek eXtended Detection and Response (XDR) ürünlerine dönüşmüştür. Gelişmiş tehditleri önlemek için bu teknolojilerin zorunlu hale getirilmesini öneriyoruz.

3. Sıfır güven mimarisi siber güvenlik alanında baskınlığını arttırmaktadır. 2020 yılında yayınlanan NIST SP 800-207 Zero Trust Architecture (Kaynak 3) dokümanı ve ardından 2022 yılında ABD Başkanlık Yönetim Ofisi tarafından yayınlanan M-22-09 numaralı Federal Zero Trust Strategy (Kaynak 4) muhtırası ile devlet kurumları ve ilintili özel şirketlere sıfır güven mimarisi zorunlu hale getirilmiştir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayınlanmış olan Bilgi ve İletişim Güvenliği Rehberinin sıfır güven ilkelerine doğru evrilmesini öneriyoruz.

Çalışmaya Katkıda Bulunan TR Cybersecurity Alliance Üyeleri:

Ahmet Özkan
Ahmet Öztoprak
Ali Tursun
Alper Şulan
Caner Dağlı
Cem Dursun
Cengiz Keskin
Cihan Yüceer
Çağrı Güven
Deniz Şener
Ekrem Kolday
Erhan Güleyüpoğlu
Ferhat Arpacı
Gökhan Ilgıt
Gürsel Arıcı
Kayıhan Altınöz
Mehmet Karadeniz
Metin Eser
Murat Zaralı
Nedim Kaya
Nusret Karakaya
Ömer Çuhadaroğlu
Özgür Orhan
Serkan Akcan
Serkan Kırmızıgül
Tonyukuk Özden
Tuncay Arslan
Yusuf Usta

Kaynak 1: https://www.cisecurity.org/insights/blog/cyber-attack-defense-cis-benchmarks-cdm-mitre-attck
Kaynak 2: https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf
Kaynak 3: https://csrc.nist.gov/pubs/sp/800/207/final
Kaynak 4: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf