BASIN BİLDİRİSİ

4 HAZIRAN 2024

Küçük ve orta ölçekli işletmeler için siber güvenlik zorlukları

Siber tehditler hızla artıyor ve **tüm işletmelerin %99'unu temsil eden Avrupalı küçük ve orta ölçekli işletmeler (KOBİ'ler**) özellikle savunmasız. Kaynak ve uzmanlık eksikliği, birçok KOBİ'yi felç edici siber saldırılara maruz bırakıyor. **2023 ENISA araştırmasına göre**, KOBİ'lerin %90'ı siber güvenlik sorunlarının ortaya çıktıktan sonraki bir hafta içinde işleri üzerinde ciddi bir olumsuz etkisi olacağını belirtirken, %57'si muhtemelen faaliyetlerini durduracaklarını veya işlerini kapatacaklarını söyledi.

2024 stratejiccybersecurity yetenek çerçevesi , şu anda küresel olarak 4 milyon nitelikli siber güvenlik uzmanı eksikliği olduğunu belirtiyor. **Avrupa Ekonomik Forumu** , yüksek vasıflı güvenlik mimarları ve mühendisleri talep edilirken, tüm rollerin derin teknik beceriler gerektirmediğini vurgulamaktadır. Birçok yönetim pozisyonu, işbirliği, eleştirel düşünme ve problem çözme gibi "yumuşak beceriler" gerektirir. Bu nedenle, siber güvenlik bilgisi ile birlikte yönetim uzmanlığına sahip profesyonellere de ihtiyaç vardır.

Bu ve diğer zorluklara yanıt olarak, Avrupa ülkelerinden 8 kuruluştan oluşan bir konsorsiyumdan oluşan ve Vilnius Üniversitesi tarafından koordine edilen uluslararası C y berA g ent projesi başlatıldı. CyberAgent projesinin amacı, KOBİ çalışanlarının siber güvenlik ve girişimcilik becerileri kazanabilecekleri bir platform oluşturmak ve kadınların bilişim sektörüne katılımını artırmaktır.

İlk proje etkinliği düzenlendi

Bu yılın mayıs ayının sonunda ilk proje etkinliği gerçekleşti. Temel amaç, Avrupalı KOBİ'lerin karşılaştığı belirli siber güvenlik konuları ve tehditleri hakkında tartışmaları teşvik etmek, proje sonuçlarını sunmak ve bunları siber güvenlik ihtiyaçlarına uyarlamaktı. Etkinliğin moderatörlüğünü STK Olemisen'in bir temsilcisi olan Karim yaptı.

Proje koordinatörü Dr. Renata Danieliene, ilgilenen kuruluşları, üyeleri proje etkinliklerine davet edilecek ve pilot siber güvenlik eğitimlerine katılacak olan projenin siber güvenlik ağına katılmaya teşvik etti. Ayrıca, "etkinliğin sadece proje yaygınlaştırma için değil, aynı zamanda deneyimleri paylaşmak ve aralarında işbirliğini teşvik etmek için de olduğunu vurguladı.
şirketler, yükseköğretim kurumları ve mesleki eğitim kurumları."

Uzmanların sunumları ve tartışmaları

KOBİ'lerin karşılaştığı mevcut siber güvenlik zorluklarına ve çözümlerine kapsamlı bir genel bakış sağlamak için çeşitli kurum ve alanlardan çeşitli siber güvenlik uzmanları davet edildi.

CyberAgent

Funded by the European Union

Romanya Ulusal Siber Güvenlik Müdürlüğü'nden Dr. Danut Maftei , Avrupa Birliği'ndeki KOBİ'lerin karşılaştığı çeşitli siber güvenlik zorluklarını sundu. "Dünyanın bazı ülkelerinde, siber tehditlerle etkin bir şekilde mücadele etmek için gerekli olan kurumlar arasında ulusal düzeyde iyi bir işbirliği eksikliği olduğunu fark ettim", diye vurguluyor Dr. Danut Maftei sunumunda.

DNSC ve UPB'den bir temsilci olan Doçent Emil Simion da eğitim ve işbirliğinin önemi hakkında konuştu. "Okullarda ve üniversitelerde eğitime dikkat etmemiz gerekiyor çünkü genç uzmanların karmaşık siber güvenlik sorunlarının üstesinden gelmeye hazırlıklı olması gerekiyor. Akademik kurumlar, araştırma ve geliştirme kurumları ve özel sektör kuruluşlarıyla işbirliği yaparak, bilgi ve deneyim alışverişini, mentorluk ve desteği, stajları vb. teşvik eden programlar oluşturmamız gerekiyor."

KOBİ'ler için pratik ipuçları

"HackerU Polska"dan Maciej Ciesla , KOBİ'lerin kendilerini mevcut siber güvenlik tehditlerinden nasıl koruyabileceklerine dair pratik ipuçları ve püf noktaları sağladı. Stratejinin ve tutarlı adımların uygulanmasının önemini vurguladı: "Önemli olan, her şeyi aynı anda yapmaya çalışmak yerine strateji ve adımların tutarlı bir şekilde uygulanmasıdır. Siber güvenlik, kuruluşun günlük operasyonlarına entegre edilmelidir." Ayrıca çalışan ve işveren eğitiminin önemini de vurguladı: "Günümüz çalışanları artık siber güvenlik hakkında bilgi sahibi olmaları gerekmediği bahanesini kullanamazlar çünkü herkes telefonları, bilgisayarları, interneti, bilgi sistemlerini ve hizmetlerini kullanıyor ve hepimiz toplu olarak kuruluşun siber güvenliğinden sorumluyuz."

Veri güvenliği ve risk yönetimi

Olemisen'den Jani Tuomilehto , şirket verileriyle ilişkili riskleri ve KOBİ'lerin alabileceği azaltma önlemlerini tartıştı: "Kuruluşun hangi verilere sahip olduğunu, nasıl kullanıldığını ve bunlara kimlerin erişimi olduğunu bilmek önemlidir. Bu, riskin yönetilmesine ve olası ihlallerin etkisinin azaltılmasına yardımcı olur."

Özet ve Tartışma

Etkinlikte, KOBİ'lerin önümüzdeki yıllarda karşılaşacakları büyük zorluklar hakkında bir tartışma yapıldı. Katılımcılar, kişisel sorumluluğun artırılması ve uyum gereksinimlerinin sıkılaştırılması konularını tartıştılar. Uzmanlar, güvenlik ve istikrarın öneminin önemli olduğunu, eğitimin ve uzmanların niteliklerinin artırılmasının bu konunun ele alınmasına yardımcı olabileceğini vurguladı.

Katılımcılar ayrıca siber güvenlik stratejilerinin KOBİ'ler için nasıl daha erişilebilir hale getirileceğini tartıştılar, tutarlı adımların uygulanmasını vurguladılar ve çok faktörlü kimlik doğrulama ve ağ güvenliği gibi temel hususlara odaklandılar. Ek olarak, kuantum teknolojisinin güvenlik üzerinde önemli bir etkiye sahip olabileceği, ancak bunun yeni kriptografik önlemlerin geliştirileceği kademeli bir süreç olacağı kaydedildi.

Bir sonraki proje etkinliğinin bu yıl sonbaharda yapılması planlanıyor. Etkinlik, ağ oluşturma ve geliştirmeye odaklanacak. En son gelişmelerden ve yaklaşan etkinliklerden haberdar olmak için sizi sosyal medyadaki CyberAgent proje haberlerini takip etmeye davet ediyoruz.

CyberAgent

Funded by the European Union

Proje koordinatörü - Vilnius Üniversitesi Kaunas Fakültesi.
Dr. Renata Danielienė, Sosyal Bilimler ve Uygulamalı Bilişim Enstitüsü. renata.danieliene@knf.vu.lt

Avrupa Birliği tarafından finanse edilmektedir. Bununla birlikte, ifade edilen görüş ve düşünceler yalnızca yazar(lar)a aittir ve Avrupa Birliği veya Avrupa Eğitim ve Kültür Yürütme Ajansı'nın (EACEA) görüşlerini yansıtmayabilir. Bunlardan ne Avrupa Birliği ne de EACEA sorumlu tutulamaz.

CyberAgent

Funded by
the European Union