Kasım 2023

CyberSecurity for VET and SMEs

AVRUPA SİBER GÜVENLİK MÜFREDATI

META4 INNOVATIONS E. U TARAFINDAN GELİŞTİRİLMİŞTİR

İŞ PAKETİ 3 – AVRUPA SİBER GÜVENLİK MÜFREDATI

Funded by the European Union

Avrupa Birliği tarafından finanse edilmektedir. Ancak ifade edilen görüş ve görüşler yalnızca yazar(lar)a aittir ve Avrupa Birliği'nin veya Avrupa Eğitim ve Kültür Yürütme Ajansı'nın (EACEA) görüşlerini yansıtmayabilir. Bunlardan ne Avrupa Birliği ne de EACEA sorumlu tutulamaz. KA220-VET-C9588303

İÇİNDEKİLER

PROJE HAKKINDA

SecureFuture – Mesleki Eğitim ve Öğretim ve KOBİ'ler için Siber Güvenlik – Aralık 2022 ile Aralık 2024 arasında uygulanacak bir Erasmus+ projesidir. Proje, tümü mesleki eğitim ve öğretim (VET) ve siber güvenlik alanlarında ilgili uzmanlığa sahip beş ülkeden altı ortaktan oluşan bir konsorsiyum tarafından yürütülmektedir.

ÜLKE	ORGANİZASYON
Türkiye	İstanbul Ticaret Üniversitesi (Koordinatör)
Türkiye	İstanbul Valiliği
Portekiz	Mindshift Talent Advisory
İspanya	Media Creativa 2020
İtalya	Pragma Engineering
Avusturya	Meta4 Innovations

SecureFuture konsorsiyumu, Avrupa Birliği'ndeki (AB) Mesleki Eğitim ve Öğretim okullarında verilen mevcut eğitimin işgücü piyasasının ihtiyaçlarını karşılamadığını veya bu düzeyde siber güvenlik eğitimi olmayan ülkelerin bulunduğunu tespit etmiştir. Ayrıca pek çok küçük ve orta ölçekli işletmenin (KOBİ) kadrosunda şirketlerini siber tehditlere karşı koruyacak nitelikli personele sahip değildir ve siber güvenlik konusunda dış yardım almak oldukça maliyetlidir.

Bu yönleri göz önünde bulundurarak proje, öğrencilerini ve çalışanlarını siber güvenlik yeterlilikleriyle donatmak isteyen mesleki eğitim sistemlerine ve KOBİ'lere rehberlik etmek için siber güvenlik konusunda bir Avrupa çerçevesi, müfredat ve eğitim içeriği geliştiriyor. Bu belge Avrupa Siber Güvenlik Müfredatına atıfta bulunmaktadır.

ÖZET

Önerilen Avrupa Siber Güvenlik Müfredatı, projenin çalışma paketi 3'ün nihai çıktısıdır: WP3 – Avrupa Siber Güvenlik Müfredatı.

WP3 lideri – Meta4 Yenilikleri e. U. – önerilen Avrupa Siber Güvenlik Müfredatının tasarımını ve geliştirilmesini kolaylaştırmak amacıyla tüm ortaklar için bir çalışma planı, yönergeler ve şablonlar hazırladı. Birbirine bağlı bir geliştirme süreci olarak, bu Avrupa Siber Güvenlik Müfredatı, tüm ortaklar tarafından ortaklaşa geliştirilen siber güvenlik konusundaki ulusal yeterliliklerin karşılaştırılması yoluyla Çerçeve tarafından şekillendirilmiştir.

Proje müfredatına ilişkin ilgili ulusal ihtiyaçlara genel bir bakış sağlamak amacıyla Temmuz 2023 ayı boyunca tüm ortak ülkelerde- Avusturya, İtalya, Portekiz, İspanya ve Türkiye 66 uzmandan oluşan bir havuzun girdilerini sağladığı Avrupa çapında bir anket gerçekleştirmiştir. Bu girdiler Meta4 tarafından özetlenmiş ve Avrupa Siber Güvenlik Müfredatının Öğrenme ünitelerini oluşturmak üzere ortaklarla paylaşılmıştır.

1. MÜFREDAT

GENEL BAKIŞ

ECVET'in ortak ülkelerdeki heterojen kullanımı ve eğitim saati başına ortalama ECVET puanı göz önüne alındığında, SecureFuture projesinin ortaklığı aşağıdaki şekilde mutabakata varmıştır:

20 saatlik eğitim = 1 ECVET puanı

Avrupa Siber Güvenlik Müfredatı, 6 ECVET puanına karşılık gelen, 120 saatlik bir süreye sahip 10 modül içermektedir.

Ünite 1: Siber Güvenlik Savunmasına Giriş

Giriş

'Siber Güvenlik Savunmasına Giriş' modülü, KOBİ'ler için siber güvenliğin temel bir araştırmasıdır. Sürekli değişen tehditler karşısında dijital sistemlerin ve verilerin korunması için hayati önem taşıyan temel kavram ve ilkelerin kapsamlı bir şekilde anlaşılmasını sağlar. Bu modül, öğrencileri siber güvenlik tehditlerine karşı savunmak ve günümüzün dinamik ortamında kritik bilgi varlıklarını korumak için gereken temel bilgi ve becerilerle donatır.

Amaç

Amaç, kursiyerlere siber tehditleri etkili bir şekilde tanımlamak, azaltmak ve bunlara yanıt vermek için temel siber güvenlik kavramları ve ilkeleri konusunda sağlam bir anlayış kazandırmaktır.

ÖĞRENME ÇIKTILARI

Bilgi	K1. Siber güvenlik ve veri korumanın temel ilkelerini anlamak. K2. Yaygın siber tehditleri ve güvenlik açıklarını tanımlamak. K3. Siber güvenliğin yasal ve etik yönlerini kavramak.	**Yetenekler**	S1. Şüpheli etkinliklere karşı ağ trafiğini analiz etme becerisi kazanır. S2. Tehditlere ve güvenlik açıklarına karşı güvenlik duvarlarını yapılandırma becerisi kazanır. S3. Güvenlik testleri ve değerlendirmeleri yapma becerisi kazanır.	**Sorumluluk ve Özerklik**	RA1. Siber güvenliğe yönelik özel bir eylem planı geliştirmek için güvenlik risklerini değerlendirin ve önceliklendirin. RA2. Kötü amaçlı yazılım veya kimlik avı gibi yaygın siber tehditlere etkili bir şekilde yanıt verin. RA3. Güvenlik olaylarının etkisini en aza indirmek için prosedürler üzerinde iş birliği yapın.

Süre

İletişim saatleri	Uygulamalı saatler	Bireysel çalışma saatleri	Değerlendirme saatleri	TOPLAM
0,5	2	9	0,5	12

Ünite 2: Veri Koruma ve Gizlilik

Giriş

Bu modül, öğrencilere dijital çağda veri güvenliği için gerekli yetkinlikleri kazandırır. Veri sınıflandırması, hassas bilgilerin sorumlu bir şekilde ele alınması, gizlilik, fikri mülkiyet ve siber savaşın karmaşıklığı dahil olmak üzere veri korumanın temel yönlerini kapsar. Etkili veri şifreleme, güvenli depolama uygulamaları ve veri ihlallerine karşı olay müdahalesinin yanı sıra GDPR ve diğer veri koruma düzenlemeleri vurgulanmaktadır. Modül, siber güvenlikte gizlilik, etik ve uyarlanabilirliğe öncelik veren tutumları teşvik ederek öğrencilerin dijital savunmaya aktif olarak katkıda bulunmalarına ve uyanık veri ve mahremiyet koruyucuları olmalarına olanak tanır.

Amaç

Öğrencileri, verileri etkili bir şekilde korumak ve yönetmek için gerekli bilgi, beceri ve tutumlarla güçlendirmek, veri koruma düzenlemelerine uygunluğu sağlamak ve siber güvenlikte gizliliği korumak.

ÖĞRENME ÇIKTILARI

Bilgi	K1. Hassas bilgiler, fikri mülkiyet ve siber savaş dahil olmak üzere veriyle ilgili kavramları tanımlamak K2. Kişisel veriler, dijital veriler ve Genel Veri Koruma Yönetmeliği (GDPR) ile ilgili veri koruma düzenlemelerini farklılaştırmak. K3. Sorumlu veri işlemeyi önceliklendiren bir zihniyet geliştirmenin önemini açıklamak.	**Yetenekler**	S1. Yeterli şifreleme tekniklerini farklı veri türleriyle ilişkilendirir. S2. Şifreleme, erişim kontrolleri ve düzenli yedeklemeler dahil olmak üzere güvenli veri depolamayla ilgili en iyi uygulamaları uygular. S3. İhlallerin ciddiyetini dikkate alarak veri ihlali yönetim planları oluşturur.	**Sorumluluk ve Özerklik**	RA1. Verilerin korunmasına ve bireysel gizlilik haklarına saygı gösterilmesine yönelik farkındalığı artırın RA2. Veri işleme ve fikri mülkiyet konularında etik bir yaklaşım benimseyin RA3. Sürekli gelişen siber güvenlik tehditlerine ve düzenlemelerine karşı dayanıklı ve uyarlanabilir bir tutum geliştirin

Süre

İletişim saatleri	Uygulamalı saatler	Bireysel çalışma saatleri	Değerlendirme saatleri	TOPLAM
0,5	2	9	0,5	12

Ünite 3: Risk Yönetimi ve Uyumluluk

Giriş

Bu modül, siber güvenlik risklerini yönetmek ve uyumluluğu sağlamak için temel yetkinlikleri kazandırır. Riskin tamamen ortadan kaldırılmasının ulaşılamaz olduğunu kabul ederek, siber risk yönetimini kurum çapındaki risk yönetimi uygulamalarına entegre eder. Bunun yerine, etkili siber risk yönetimi programları aracılığıyla tehdit etkilerini azaltmaya odaklanır. Modül, öğrencilere uluslararası kabul görmüş standartları, özellikle de Bilgi Güvenliği Yönetim Sistemini (ISMS) tanıtır ve uyumluluk için temel adımları ve kontrol listelerini ana hatlarıyla belirtir. Modül, bilgi ve becerilere ek olarak, risk analizi, tanıma ve azaltma konularında BGYS uyumluluk şemalarının ve tavsiyelerinin uygulanmasıyla ilgili tutumların geliştirilmesinin altını çizerek öğrencilere bilgi güvenliğine sistemik bir yaklaşımı teşvik ederek siber güvenlik tehditlerini proaktif bir şekilde ele alma ve yönetme konusunda güçlendirir.

Amaç

Öğrencileri, siber güvenliğe yönelik uluslararası uyumluluk kurallarına da atıfta bulunulan risk yönetimi metodolojilerini etkili bir şekilde uygulamak için gerekli bilgi, beceri ve tutumlarla güçlendirmek.

ÖĞRENME ÇIKTILARI

Bilgi	K1. Bilgi Güvenliği Yönetim Sistemi bileşenlerini ve gereksinimlerini tanımlamak. K2. Bilgi Güvenliği Yönetim Sisteminin bir fonksiyonu olarak Bilgi Riski Yönetimini tanımlamak. K3. Siber Güvenlik uyumluluk kurallarına yaklaşımı açıklamak.	**Yetenekler**	S1. Bilgi Güvenliği Yönetim Sisteminin ana bileşenlerini tanımlar S2. KOBİ'lere uygulanan Tasarım Risk Yönetimi planlarını dizayn eder. S3. Siber Güvenlik uyumluluk kuralları gerekliliklerini inceler.	**Sorumluluk ve Özerklik**	RA 1. KOBİ'lerin Bilgi Güvenliği Yönetim Sisteminin tanımlanmasında işbirliği yapın. RA2. Risk Yönetimi sürecine uyun. RA3. Siber Güvenlik uyumluluk kurallarının benimsenmesiyle ilgilenin.

Süre

İletişim saatleri	Uygulamalı saatler	Bireysel çalışma saatleri	Değerlendirme saatleri	TOPLAM
0,5	2	9	0,5	12

Ünite 4: Sosyal Mühendislik ve Kimlik Avı Farkındalığı

Giriş

Bu modül , dijital olarak bağlantılı dünyamızda hayati önem taşıyan sosyal mühendislik ve kimlik avı farkındalığına odaklanır. Bu konular, bulut sistemlerinin işletmeler üzerindeki dönüştürücü etkisi kadar kritik öneme sahiptir. Ünitenin sonunda öğrenciler sosyal mühendisliği tanımlayacak, motivasyonlarını (mali kazanç ve veri hırsızlığı gibi) kavrayacak ve siber suçlular tarafından kullanılan çeşitli kimlik avı tekniklerini ve saldırı vektörlerini tanıyacaklardır. Bu onların tehdit tespit ve müdahale yeteneklerini geliştirmelerine yardımcı olacaktır. Öğrenciler ayrıca sorumlu siber güvenlik uygulamalarını teşvik ederek sosyal mühendislik saldırılarının yasal ve etik sonuçlarını da kavrayacaklardır. Ünite, etik farkındalığı aşılamakta, olaylara müdahalede iş birliğini teşvik etmekte ve yasal uyumluluğu vurgulamaktadır. BT profesyonellerine, işletme sahiplerine, mesleki eğitim öğrencilerine veya güvenli bir dijital gelecek için siber güvenlik bilgisini güçlendirmek isteyen herkesi hedeflemektedir.

Amaç

Bu öğrenme ünitesi, katılımcıları sosyal mühendisliği tanımlamak, kimlik avı tekniklerini belirlemek ve bunların yasal ve etik sonuçlarını etkili bir şekilde anlamak için bilgi, beceri ve etik tutumlarla donatmayı amaçlamaktadır.

ÖĞRENME ÇIKTILARI

Bilgi	K1. KOBİ'ler Bağlamında Sosyal Mühendisliği ve Motivasyonlarını tanımlamak. K2. KOBİ'leri savunmasız bırakan Kimlik Avı Tekniklerini ve Saldırı Vektörlerini belirlemek. K3. KOBİ'ler Bağlamında Sosyal Mühendisliğin Yasal ve Etik Sonuçlarını hatırlamak.	**Yetenekler**	S1. Sosyal mühendislik saldırılarını yönlendiren temel motivasyonları tanımlamak S2. Hedef odaklı kimlik avı, vishing (sesli kimlik avı) ve bahane uydurma gibi yöntemleri tanımak S3. Hem failler hem de mağdurlar için olası sonuçları anlamak	**Sorumluluk ve Özerklik**	RA1. Bilginin sorumlu ve ilkeli kullanımına yönelik sosyal mühendislik amaçlarını tanımlarken etik farkındalığı teşvik edin. RA2. Saldırı tekniklerini ve vektörlerini belirlerken kimlik avı tehditlerini azaltmak için ekiplerle iş birliği yapın. RA3. Yasalara bağımsız olarak uyun, sosyal mühendislik eylem ve uygulamalarında yasallığı sağlayın.

Süre

İletişim saatleri	Uygulamalı saatler	Bireysel çalışma saatleri	Değerlendirme saatleri	TOPLAM
0,5	2	9	0,5	12

Ünite 5: KOBİ'ler için Bulut Güvenliği

Giriş

Bu ünite, esneklik, ölçeklenebilirlik ve maliyet verimliliği açısından bu sistemlere giderek daha fazla güvenen KOBİ'ler için bulut sistemlerinin sunduğu benzersiz güvenlik zorluklarını ele almaya odaklanmaktadır. KOBİ'lere bulut güvenliğini etkili bir şekilde yönetmek için gerekli bilgi ve becerileri sağlamak üzere tasarlanmıştır. Ünite, KOBİ'lerin özel ihtiyaçlarına ve kısıtlamalarına göre uyarlanmış olup, riskleri azaltmak, hassas bilgileri korumak ve sektör düzenlemelerine uyumu sağlamak için pratik bilgiler ve eyleme dönüştürülebilir stratejiler sunmaktadır. Öğrenciler bulut güvenliğinin temel ilkelerini ve en son teknolojileri keşfedecek ve güvenlik önlemlerinin uygulanmasında uygulamalı deneyim kazanacaklardır. İster bir işletme sahibi ister BT uzmanı, Mesleki Eğitim öğrencisi veya bulut güvenliği bilgilerini geliştirmek isteyen biri olsun, bu müfredat, öğrencileri KOBİ'lerinin dijital geleceğini etkili bir şekilde güvence altına almak için gereken araçlarla donatır.

Amaç

Bu ünite, öğrencilerin bir KOBİ için bulut sistemlerini kullanmanın etkisini en üst düzeye çıkarmak için avantajlar, olası riskler ve talimatlar hakkında fikir sahibi olmalarını sağlamayı amaçlamaktadır.

ÖĞRENME ÇIKTILARI

Bilgi	K1. Bir KOBİ için bulut sistemlerini kullanmanın faydalarını tanımlamak K2. Bulut sistemlerini kullanmanın olası risklerini tanımlamak ve azaltmak. K3. KOBİ'lerin bulut bilişim güvenliği için dikkate alınabilecek önleyici adımları özetlemek.	**Yetenekler**	S1. Bulut bilişimin KOBİ'ler tarafından hangi açıdan ve nasıl kullanılabileceğini analiz eder. S2. Güvenlikle ilgili sorguları risk yönetimi bağlamında sunabilir ve çözümler önerir. S3. Bulut sistemlerinin kullanımını etkileyebilecek farklı türdeki yasal gereklilik türlerini örneklendirir.	**Sorumluluk ve Özerklik**	RA1. AB kişisel verileri ve ulusal koruma mevzuatı ile uyumlu bir bulut güvenliği sağlayın RA2. Bulut sistemine sahip olma konusunda örnek bir senaryo sağlamak için meslektaşlarınızla iş birliği yapın RA3. Bir satın alma işleminde güvenlik fırsatlarını değerlendirmek için bir ekibe liderlik edin

Süre

İletişim saatleri	Uygulamalı saatler	Bireysel çalışma saatleri	Değerlendirme saatleri	TOPLAM
0,5	2	9	0,5	12

Ünite 6: Ağ Güvenliğinin Temelleri

Giriş

Ağ güvenliği, siber tehditlere karşı savunma yapmak isteyen KOBİ'ler için çok önemli bir husustur. Fiziksel ve yazılım tabanlı önlemleri içeren bütünsel bir yaklaşımı içerir ve kuruluş çapında bir anlayış gerektirir. Öğrenciler, kavramsal kavrama ve kişilerarası becerileri kapsayan, önlemlere ilişkin derinlemesine bilgi sahibi olacaklardır. KOBİ'lerin ağ güvenliğini yönetmeleri için koruyucu eylemler gerçekleştirebilecek özel ekipler oluşturmak da dahil olmak üzere mevcut önlemler hakkında bilgi edineceklerdir. Bu ünite, katılımcılara ağ güvenliğinin karmaşık alanında gezinme uzmanlığı vererek şirketlerini ve operasyonlarını gelişen siber tehdit ortamından etkili bir şekilde korumalarını sağlar.

Amaç

Bu ünite, öğrencilere KOBİ'ler için ağ güvenliği ve işlerini KOBİ'lerin güvenliğine doğru nasıl yönlendirecekleri konusunda temel bir anlayış sağlamayı amaçlamaktadır.

ÖĞRENME ÇIKTILARI

Bilgi	K1. Ağ güvenliğinin temel terimlerini ve kavramlarını açıklamak K2. Ağ iletişiminde kullanılan temel topolojileri ve stratejileri hatırlamak K3. Fiziksel ağ bağlantı elemanlarını ve fiziksel güvenlik prosedürlerini tanımlamak	**Yetenekler**	S1. Ağ güvenliğinin bir KOBİ için neden önemli olduğunu tartışır S2. Ağ güvenliğindeki olası riskleri ve olası çözümleri gösterebilir S3. Potansiyel ağ tehditlerini ve bir KOBİ'nin bunlara nasıl tepki vermesi ve bunları önlemesi gerektiğini ana hatlarıyla belirtir.	**Sorumluluk ve Özerklik**	RA1. Ağ güvenliği için oluşturulmuş bir ekibe liderlik edin RA2. Bir şirketin ağ güvenliğini iş planına nasıl entegre edebileceğine dair öneriler sunun. RA3. Ağ güvenliği prosedürlerinin uygulanmasını doğrulayın ve izleyin.

Süre

İletişim saatleri	Uygulamalı saatler	Bireysel çalışma saatleri	Değerlendirme saatleri	TOPLAM
0,5	2	9	0,5	12

Ünite 7: Güvenli Yazılım Geliştirme

Giriş

Güvenli yazılım geliştirme, artan siber tehditler karşısında son derece önemlidir. Tasarım ve kodlamadan test, dağıtım ve bakıma kadar tüm yazılım geliştirme döngüsü boyunca güvenlik uygulamalarının yerleştirilmesini gerektirir. Amacı verileri korumak, kullanıcı gizliliğini korumak ve yazılım sistemi bütünlüğünü ve kullanılabilirliğini sağlamaktır. Temel ilkeler, birden fazla güvenlik katmanıyla derinlemesine savunmayı, minimum erişim için en az ayrıcalığı ve projenin başlangıcından itibaren tasarım gereği güvenliği kapsar. Sızma testleri ve kod incelemeleri de dahil olmak üzere düzenli testler esastır. Güvenli dağıtım, bakım ve olaylara müdahale, sürekli güvenlik için çok önemlidir. Eğitim ve farkındalık, destekleyici kaynaklarla birlikte kurumsal güvenliği daha da artırır. Riskleri azaltan ve kullanıcı güvenini koruyan güvenli yazılım geliştirme, günümüzün tehdit ortamında vazgeçilmezdir.

Amaç

İhlal ve siber saldırı risklerini en aza indirirken ve bakım, test ve eğitim sağlarken güvenli yazılım geliştirme uygulamalarını, sistemleri, hassas verileri ve kullanıcı gizliliğini korumayı öğrenin.

ÖĞRENME ÇIKTILARI

Bilgi	K1. Güvenli kodlama uygulamalarını, ortak güvenlik tehditlerini ve güvenlik standartlarını ve çerçevelerini tanımlamak. K2. Güvenli geliştirme yaşam döngüsünü ve yapılandırma yönetimini, güvenli dağıtım ve bakımını öğrenmek K3. Güvenlik Açığı değerlendirmesini ve sızma testini, şifrelemeyi ve kriptografiyi, güvenli API'leri ve entegrasyonları belirlemek	**Yetenekler**	S1. Güvenli kodlamayı, güvenlik açığı değerlendirmesini, güvenlik testini, şifrelemeyi ve kriptografiyi deneyimler S2. Güvenli yapılandırma yönetimi, dağıtım ve bakım, güvenli API tasarımı oluşturur S3. Uyumluluk ve gizlilik düzenlemelerini iyileştirin, sürekli öğrenir	**Sorumluluk ve Özerklik**	RA1. Geliştiricilerin kodlama uygulamalarında güvenliğe öncelik verme sorumluluğuna sahip olduğunu dikkate alın RA2. Yazılım geliştirme sürecinde güvenlikle ilgili konularda kararlar alın. RA3. Güvenlik gereksinimlerinin uygun şekilde karşılandığından emin olmak için geliştirme süreci sırasında güvenlik uzmanlarıyla işbirliği yapın.

Süre

İletişim saatleri	Uygulamalı saatler	Bireysel çalışma saatleri	Değerlendirme saatleri	TOPLAM
0,5	2	9	0,5	12

Ünite 8: Güvenli Uç Nokta Koruması

Giriş

Günümüzün birbirine bağlı dünyasında dizüstü bilgisayarlar, masaüstü bilgisayarlar, mobil cihazlar ve sunucular dahil uç noktaları siber saldırılardan korumak çok önemlidir. Güvenli uç nokta koruması, bu cihazları kötü amaçlı yazılımlardan, fidye yazılımlarından, kimlik avından ve yetkisiz erişimden korumak için çok katmanlı bir savunma stratejisinin uygulanmasını gerektirir. Bu, güçlü antivirüs ve kötü amaçlı yazılımdan koruma yazılımlarının dağıtılmasını, gelişmiş tehdit algılama ve önleme mekanizmalarından yararlanılmasını, sıkı erişim kontrolleri ve kimlik doğrulama önlemlerinin uygulanmasını ve yazılım ve işletim sistemlerinin düzenli olarak güncellenmesini içerir. Güvenli uç nokta koruması, veri ihlallerini önlediği, hassas bilgilere yetkisiz erişimi önlediği ve iş sürekliliğini koruduğu için her büyüklükteki ve sektördeki kuruluşlar için kritik öneme sahiptir. Kuruluşlar, uç noktaları güçlendirerek siber saldırı riskini azaltabilir, sektör düzenlemelerine uyabilir ve itibarlarını ve müşterilerinin güvenini koruyabilir.

Amaç

Dizüstü bilgisayarları, masaüstü bilgisayarları, mobil cihazları ve sunucuları kötü amaçlı yazılımlara, fidye yazılımlarına, kimlik avına ve yetkisiz erişime karşı korumayı, veri ihlallerini ve operasyonel aksaklıkları azaltmayı, uyumluluğu sağlamayı ve güveni korumayı öğrenmek.

ÖĞRENME ÇIKTILARI

Bilgi	K1. Uç nokta güvenliğini ve güvenli uç nokta korumasına genel bakışı anlamak K2. Güvenli uç nokta koruması, Antivirüs, Güvenlik Duvarı ve Şifrelemenin Temel bileşenlerini tanımlamak K3. Güvenli uç nokta koruması, yama yönetimi, tehdit tespiti ve kullanıcı eğitiminin uygulanmasına yönelik en iyi uygulamaları belirlemek	**Yetenekler**	S1. Etkili azaltma için kötü amaçlı yazılım, fidye yazılımı ve kimlik avı tehditlerini analiz edebilir ve bunlara yanıt verebilir. S2. Etkili dağıtım ve operasyon için uç nokta güvenlik araçlarını (antivirüs, güvenlik duvarları, şifreleme) yönetir ve yapılandırır. S3. Uç nokta güvenliği için yama yönetimi, erişim kontrolleri, veri şifreleme ve kullanıcı farkındalığı özelliklerine sahiptir.	**Sorumluluk ve Özerklik**	RA 1. Tehditlere ve güvenlik açıklarına etkili bir şekilde karşı koymak için uç noktaları antivirüs, güvenlik duvarları ve şifrelemeyle koruyun. RA2. Uç nokta güvenliği sorumluluğunu üstlenin, riskleri tanımlayın, azaltın, değerlendirmeler yapın ve güvenliği sürdürün. RA3. Güvenlik olaylarına hızlı bir şekilde müdahale edin, araştırın, adli tıp yürütün, iyileştirme uygulayın, tekrarları önleyin.

Süre

İletişim saatleri	Uygulamalı saatler	Bireysel çalışma saatleri	Değerlendirme saatleri	TOPLAM
0,5	2	9	0,5	12

Ünite 9: Olay Yönetimi ve Müdahale

Giriş

Olay Yönetimi ve Müdahale, çok çeşitli aksaklıkları ve tehditleri azaltmak için gereklidir. Amacı, operasyonları kesintiye uğratabilecek veya bir kuruluşun varlıklarına, itibarına ve paydaşlarına zarar verebilecek olayları etkili bir şekilde belirlemek, analiz etmek ve bunlara yanıt vermektir. Bu olaylar siber saldırıları, veri ihlallerini, doğal afetleri, kazaları ve halk sağlığıyla ilgili acil durumları kapsamaktadır. Ana amaç, yapılandırılmış bir çerçeveyi takip ederek etkiyi en aza indirmek, operasyonları eski haline getirmek ve gelecekteki olayları önlemektir. Başarılı olay yönetimi aynı zamanda ekipler ve paydaşlar arasında açık iletişim ve iş birliğini de gerektirir. Sağlam bir strateji, kuruluşların riskleri proaktif bir şekilde ele almasına, dayanıklılığı artırmasına, kesinti süresini azaltmasına, verileri korumasına, düzenlemelere uymasına ve itibarını korumasına olanak tanır.

Amaç

Genel istikrar ve güvenlik için hızlı tespit , kaynakların harekete geçirilmesi, koordineli müdahale ve normal operasyonların hızlı bir şekilde eski haline getirilmesi dahil olmak üzere olayın etkisini en aza indirmek için etkili bir şeklide yanıt vermeyi öğretmek.

ÖĞRENME ÇIKTILARI

Bilgi	K1. Olay Tespit ve Raporlama, Olay Değerlendirme ve Analizinin hazır hale getirmek K2. Olay Müdahale Planlaması ve Hazırlık, Olay Sınırlaması ve Azaltmak K3. Olay İletişimi ve Koordinasyonunu, Olay Kurtarmayı ve Öğrenilen Dersleri organize etmek.	**Yetenekler**	S1. Güçlü problem çözme becerilerini kullanarak olayları analiz eder nedenlerini belirler ve uygun müdahale stratejilerini seçer. S2. Olay yönetimi ve müdahale için etkili iletişim kurar. S3. Etkin olay yönetimi ve müdahalede olay tespiti için teknik bilgiyi uygular.	**Sorumluluk ve Özerklik**	RA1. Bir kuruluş içinde meydana gelen olayları derhal tespit etmek ve önceliklendirmek için hazırlanmıştır. RA2. Olaylara müdahaleyi koordine etme ve yürütme sorumluluğunu üstlenin. RA3. Olayların belgelenmesi ve raporlanması sorumluluğunu üstlenin

Süre

İletişim saatleri	Uygulamalı saatler	Bireysel çalışma saatleri	Değerlendirme saatleri	TOPLAM
0,5	2	9	0,5	12

Ünite 10: İş Sürekliliği ve Felaket Kurtarma

Giriş

İş Sürekliliği ve Felaket Kurtarma (BCDR), bir kuruluşun risk yönetimi stratejisinin ayrılmaz bir parçasıdır ve kritik iş operasyonlarının sürekliliğini ve kesinti zamanlarında sistem ve verilerin kurtarılmasını sağlar. İş Sürekliliği, proaktif planlamayı, hayati süreçleri belirlemeyi, riskleri değerlendirmeyi ve bir kesinti sırasında ve sonrasında iş operasyonlarını sürdürmek için stratejiler geliştirmeyi içerir. Felaket Kurtarma, yedekleme ve kurtarma planları, esnek BT sistemleri ve normal operasyonları hızlı bir şekilde geri yükleme prosedürlerini içeren teknik yönlere odaklanır. Her iki BCDR unsuru da bir kuruluşun varlıklarının, bağımlılıklarının ve risklerinin kapsamlı bir şekilde anlaşılmasını gerektirir. Departmanlar arasında iş birliği ve koordinasyon, rol netliği, iletişim, eğitim ve test hayati öneme sahiptir. Etkili BCDR planları kesinti etkisini en aza indirir, güveni korur ve uzun vadeli operasyonel esneklik sağlar.

Amaç

Kritik iş operasyonlarını güvence altına almayı, kesinti etkilerini en aza indirmeyi, riskleri tanımlamayı, kurumsal dayanıklılığı artırmak ve uzun vadeli sürdürülebilirliği sağlamak için planlar geliştirmeyi ve test etmeyi öğrenmek

ÖĞRENME ÇIKTILARI

Bilgi	K1. Risk Değerlendirmesi ve İş Etki Analizi, İş Sürekliliği Planlamasını tanımlamak K2. BT Felaket Kurtarma Planlaması ve Kriz Yönetiminin temel unsurlarını tanımlamak K3. İş operasyonlarının sürekliliğiyle ilgili Yedekleme ve Kurtarma Stratejileri konusunda farkındalık oluşturmak.	**Yetenekler**	S1. Kritik iş operasyonlarına yönelik potansiyel tehditleri ve güvenlik açıklarını belirlemek için risk değerlendirmeleri ve analizleri yapabilir. S2. Kapsamlı iş sürekliliği ve felaket kurtarma planları oluşturur. S3. Kritik operasyonların sürekliliğini ve sistem ve verilerin zamanında kurtarılmasını sağlamak için gereken prosedürleri ve kaynakları listeler.	**Sorumluluk ve Özerklik**	RA 1. Kritik iş operasyonları ve BT sistemlerine yönelik potansiyel riskleri ve güvenlik açıklarını belirleme ve değerlendirme sorumluluğu. RA2. Kapsamlı iş sürekliliği ve felaket kurtarma planlarının uygulanması için hazırlanmıştır. RA3. Etkinliğini sağlamak için iş sürekliliği ve felaket kurtarma planlarını düzenli olarak izleyin ve test edin.

Süre

İletişim saatleri	Uygulamalı saatler	Bireysel çalışma saatleri	Değerlendirme saatleri	TOPLAM
0,5	2	9	0,5	12

2. AÇIKLAMALAR

Erasmus+ projesi SecureFuture kapsamında geliştirilen Avrupa Siber Güvenlik Müfredatı, ülkelerinde Siber Güvenlik alanında çalışan 66 profesyonelle yapılan ulusal istişarelerin ardından proje ortakları tarafından sağlanan girdilerle hassas bir şekilde hazırlandı.

Aşağıdaki parametreleri dikkate alır:

- Eğitim içeriğinin, yeterlilik birimleri ve ilgili içerikler olarak on alana modüler bir şekilde dağıtılması;
- On öğrenme biriminin her biri için bir tabloda derlenen bir dizi bilgi, beceri, sorumluluk ve özerklik;
- 120 saatlik eğitime karşılık gelen 10 ünite setine 6,0 ECVET puanı atanması.

Bu Müfredat, WP4 – SecureFuture Eğitim İçeriği'nde tanımlandığı şekilde Avrupa Siber Güvenlik Eğitim İçeriğinin geliştirilmesinin temelini oluşturacaktır.

Avrupa Yeterlilikler Çerçevesi, Eğitim Müfredatı ve Eğitim İçeriği birlikte, Avrupa ülkelerinin mesleki eğitim öğrencileri ve KOBİ çalışanları- projenin ana hedef grupları- için siber güvenlik eğitimi konusundaki ihtiyaçlarını karşılama ve böylece Avrupa KOBİ'lerini siber tehditlerden korumak için iyi eğitimli siber güvenlik uzmanları hazırlama konusunda güçlü bir potansiyele sahip yenilikçi bir değer önerisidir.