Co-funded by the
Erasmus+ Programme
of the European Union

InCyT Eğitim Modülleri

Çalışanlar için Bilgi Güvenliği **Ünite 1 Hafta 1** **birim adı: Tanıtım Web Semineri**	
Öğrenme aktiviteleri	❑ **Web Semineri** ❑ **Egzersizler** ❑ **Atölye** ❑ **Sunum** ❑**Diğer**
Öğrenme Sorumlusu	• Gabriel Vladut • Valentin Istratie
Öğrenme Etkinliği Hedefleri	1. Erasmus+ InCyT projesi hakkında tanıtım 2. Hedefler 3. Sonuçlar ve ürünler 4. Siber saldırılara karşı kendinizi nasıl korursunuz? 5. Eğitim ve mentorluk 6. Sosyal mühendislik 7. Sosyal Ağ (Sosyal Medya)
Kazanılacak Beceriler	• TS3 Ağ Güvenliği • TS4 Sızma (istismar edilebilir güvenlik açıkları) testi • SS3 Bilişsel ve davranış analizi
Öğrenme faaliyetinin süresi	2 hafta
Öğrenme Gereksinimler	***İhtiyaç duyulan şey?*** • Erasmus+ InCyT projesi / hedefleri / Sonuçları ve ürünleri hakkında bilgi edinmek • Siber saldırılara karşı kendinizi nasıl korursunuz? • Eğitim ve mentorluk • Sosyal mühendislik / Sosyal Ağ (Sosyal Medya)

Co-funded by the
Erasmus+ Programme
of the European Union

Modül hakkında kısa bilgi

Tanım
InCyT, Mesleki Eğitim ve şirketlere, siber saldırılardan kaçınmak için profesyoneller için değil, profesyoneller için siber güvenlikte gerekli olan yeterlilikleri ve becerileri tanımlamaları için bir mekanizma sağlayan bir eğitim metodolojisi olan bir Çerçeve oluşturmayı amaçlayan bir Erasmus + projesidir. NIST'in Ulusal Siber Güvenlik Eğitimi Girişimi (NICE), "siber güvenlik çalışması için gerekli görevleri yerine getirmek için bilgi, beceri ve yeteneklere sahip kişi" eksikliğini gidermeye yönelik çok önemli bir adım atılması gerektiğinin altını çizmektedir. Böyle bir iş gücü, "bilgili ve deneyimli insanlardan oluşan teknik ve teknik olmayan rolleri" içerecektir. Proje bu bağlamda bazı çözümler uygulamak isteyecektir. Öncelikli amacı, Mesleki Eğitim ve şirketlere siber saldırılardan kaçınmak ve bu durumu iyileştirmelerine yardımcı olmak amacıyla profesyoneller için değil, profesyoneller için siber güvenlikte gerekli olan dijital boşlukları ve diğerlerini açıklamak için bir mekanizma sağlayan bir çerçeve geliştirmektir. Proje, özellikle siber güvenlik alanında disiplinler arası eğitim ve mentorluk programlarının avantajlarını göz önünde bulundurarak geliştirecek ve KOBİ'ler için e-mentorluk ile desteklenen dijital disiplinler arası eğitim programlarını test edecek ve MEÖ'ye uyarlayacaktır. Eğitimciler, araştırmacılar ve bilgi teknolojilerini kullanan kişiler arasında işbirliği ve iletişim gereklidir. Bir sorun, şirketlerin, özellikle daha az kaynağa sahip olan KOBİ'lerin, çalışanlarının yeterliliklerini ve beceri boşluklarını değerlendirmeye, mevcut durumu değerlendirme yöntemlerine ve çalışanlarına yeniden beceri kazandırmak için eğitim olanaklarını kullanmaya ihtiyaç duymalarıdır. Öğrenciler, ilgili metni okuyarak, akışlı web seminerlerini izleyerek ve alıştırmaları kendi hızlarında çözerek bu tür yönler hakkında bilgilendirilebilir. Tüm bu belgeler dijital interaktif proje platformunda yer almaktadır. Öğrenciler cevaplarını öz-değerlendirme alıştırmalarında test edebilirler. Diğer alıştırmalardaki cevaplar ilgili tartışma forumunda saklanmalı ve haftada bir düzenlenen ortak toplantıda mentor ile tartışılmalıdır. Öğrenen, özellikle toplantılar sırasında diğerleriyle ve mentorla işbirliği içinde çalışabilir. Eğitimin yansıtılması ve değerlendirilmesi için önemli olan e-portföy geliştirmeleri için desteklenecekleridir.

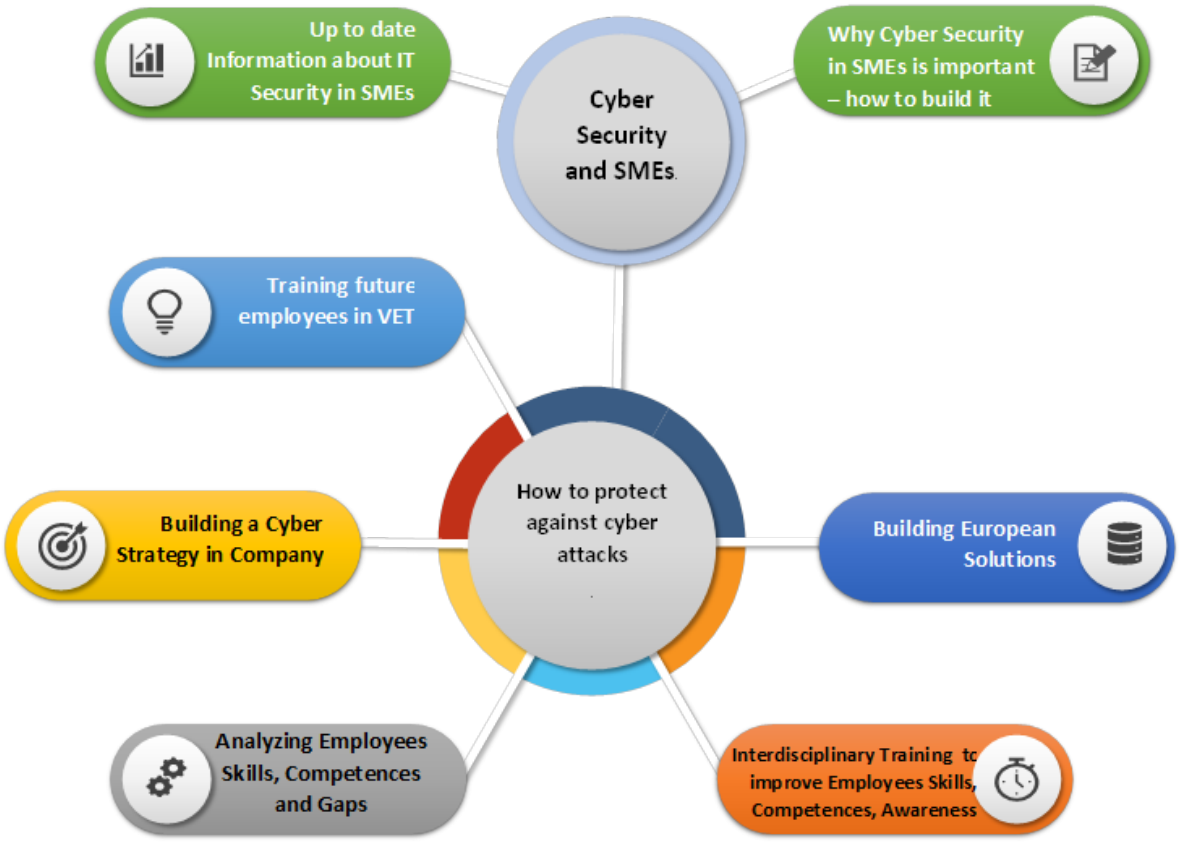
Co-funded by the
Erasmus+ Programme
of the European Union

Öğrenme Materyali İçeriği

Yetkinlik Çerçevesi

Projemizde 3 adet ulusötesi toplantı olacak. Projenin 3., 13. ve 20. aylarında planlanmıştır. 24 aylık bir projeyi yürütmek için 3 toplantının yeterli olmayacağını düşündüğümüz için bazı ek proje toplantıları yapılacaktır. Bu toplantılar çevrim içi olarak yapılır ve her ay düzenli olarak yapılır. Proje üst yönetim ekibi bu projeleri organize edecektir.

Projeler, proje koordinatörü, WP lideri tarafından yönetilecektir. Projemizde 7 adet çoğaltıcı etkinlik olacaktır. Her ortak kurum, proje fikrini kendi ülkesinde yaygınlaştırmak ve geliştirilen ürünleri paylaşmak için bu etkinlikleri düzenleyecektir. Her ortak kurum kendi ülkesinde Siber Güvenlik etkinliğinde KOBİ çalışanları ve öğretmenleri için Disiplinlerarası Eğitim yürütecektir .



InCyT projesi tarafından desteklenen faaliyetler

hedefler

InCyT projesi bazı çözümleri uygulamak isteyecektir :

- Mesleki eğitim ve şirketlere, siber saldırıların yanı sıra dijital boşluklar ve diğer saldırılardan

kaçınmak için profesyoneller için değil, profesyoneller için siber güvenlikte gerekli olan yeterlilikleri ve becerileri tanımlama mekanizması sağlayan bir Çerçevenin geliştirilmesi.

- Özellikle siber güvenlik alanında disiplinler arası eğitim ve mentorluk programlarının avantajlarını göz önünde bulunduran proje, KOBİ'ler için desteklenen dijital disiplinler arası eğitim programlarını ve işbirlikçi bir e-Öğrenim platformunu geliştirecek ve test edecektir.
- VET için uyarlayın.
- Bir Avrupa aktarılabilirlik modeli geliştirin
- Proje, özellikle siber güvenlik alanında disiplinler arası eğitim ve mentorluk programlarının avantajlarını göz önünde bulundurarak geliştirecek ve KOBİ'ler için e-mentorluk ile desteklenen dijital disiplinler arası eğitim programlarını test edecek ve MEÖ'ye uyarlayacaktır.

Projenin çıktıları şöyle olacaktır:

- Uygulama için Metodolojik Çerçeve
- Mevcut ve takip edilen eğitim (kurslar)
- Disiplinler arası ve mentorluk kullanarak bunların iyileştirilmesi için fırsatlar.
- Öğrenme ve mentorluk metodolojisi

Ürünler :

1. Çerçeve

2. KOBİ'ler için mentorluk ve MEÖ özel kursu için uyarlanmış bir metodoloji ile desteklenen dijital bir Disiplinler arası siber güvenlik eğitim materyali.

3. Eğitimi destekleyecek bir dijital platform

4. Disiplinlerarası becerilerin KOBİ ve KDV için nasıl avantajlar sağladığını rapor edin.

5. Test edilen disiplinler arası eğitim ve mentorluk için Avrupa aktarılabilirlik modeli

Ortaklar : Almanya (koordinatör), Türkiye, Polonya, İtalya, Avusturya, Danimarka, Romanya.

aktiviteler

- Siber Güvenlik için Metodolojik Çerçeve - Lider Kuruluşlar : IAT, Almanya, İtalya
- Disiplinlerarası Dijital Siber Güvenlik Eğitim Materyali - Lider Kuruluş : St. Pölten University of Applied Sciences, Avusturya
- Siber Güvenlik için ICT Platformu - Lider Kuruluş : IPA, Romanya
- Siber Güvenlik için Metodolojik Model - Lider Kuruluş : Politechnik University, Polonya

- Aktarılabilirlik Modeli - Lider Kuruluş : Avrupa Eğitim Merkezi Kopenhag, Danimarka
- Çoğaltan Etkinlikler - Lider Kuruluş : Türkiye

Siber saldırılara karşı kendinizi nasıl korursunuz?

Dijital ekonomi öncelikle verilere dayalıdır. Endüstri 4.0, siber-fiziksel sistemler ve Nesnelerin İnterneti çağında, giderek daha fazla ürün ve süreç dijitalleşiyor. Bu verilerin ve ilgili bilgi işleme sistemlerinin korunması anlamına gelen siber güvenlik, bugün ekonomi tarihinin herhangi bir zamanından daha önemlidir.

Örneğin veri kayıtlarının hatalı, eksik veya hiç mevcut olmaması, sistemler arası veri senkronizasyonunun bozulması, BT sistemlerinin hatalı çalışması veya tamamen arızalanması gibi durumlarda iş süreçleri önemli ölçüde kesintiye uğrayabilir, yavaşlayabilir ve hatta tamamen engellenebilir.

Özellikle KOBİ'ler, bu konularla ilgili suç faaliyetlerinin hedefidir. Büyük şirketlerin aksine kaynakları sınırlıdır ve bilgisayar korsanları bunu bilir! KOBİ'ler Avrupa'da ekonominin bel kemiğidir, yani Almanya'daki şirketlerin %99'undan fazlası KOBİ'dir.

İşgücünün yarısından fazlası KOBİ'ler tarafından istihdam edilmektedir. Bu nedenle, KOBİ'lerin siber saldırılardan kaçınmasına yardımcı olmak gereklidir .

Siber Güvenlik Eğitimi Girişimi, "siber güvenlik çalışmaları için gerekli görevleri yerine getirecek bilgi, beceri ve yeteneklere sahip bireyler" eksikliğini gidermek için kritik bir adım atılması gerektiğine işaret ediyor.

Böyle bir grup, "bilgi ve deneyime sahip çalışanlar tarafından doldurulan teknik ve teknik olmayan işlevleri" içerir.

Ancak gerekli disiplinler arası becerilere sahip bir iş gücü oluşturmak ve eğitimciler, araştırmacılar ve bilgi teknolojilerini kullanan kişiler arasındaki iletişim sorununu çözmek zordur.

Bu gruplar arasında işbirliği ve iletişim gereklidir.

Bir sorun, şirketlerin, özellikle daha az kaynağa sahip olan KOBİ'lerin, mevcut durumu iyileştirmek için dijital yöntemler kullanarak ve çalışanlarına yeniden beceri kazandırmak için eğitim fırsatları organize ederek, çalışanlarının becerilerini ve eksikliklerini değerlendirmek için yardıma ihtiyaç duymalarıdır.

Eğitim ve mentorluk

Geleceğin girişimcileri de dahil olmak üzere girişimciler, disiplinler arası öğrenmeyi gerektiren farklı sektörlerden bilgileri anlama ve bütünleştirme becerisine ve karmaşık düşünme biçimlerine ihtiyaç duyarlar.

Karmaşık mühendislik problemleri neredeyse doğal bir şekilde disiplinler arası bir durum yaratmayı gerektirir.

Disiplinler arası bir yaklaşımda, öğrenciler farklı disiplinlerden ve alanlardan gelen bilgileri entegre etmelidir.

Disiplinler arası bir anlayış geliştirirler, uzmanlık alanlarını ve disipline özgü düşünme biçimlerini entegre etmeyi öğrenirler.

Bu, bilişsel becerileri ve eleştirel düşünmeyi tek bir disiplin aracından daha fazla artırır.

Sosyal mühendislik

- saldırganın ilgisini çekecek verilere, belgelere ve bilgilere erişim elde etmek için (genellikle psikolojik yöntemler kullanarak) insanları manipüle etmek anlamına gelir.
- günümüzde bilgi güvenliğine yönelik ana tehditlerden biridir ve etkili bir siber suç biçimidir.
- veri ihlalleri gibi diğer tüm saldırı türlerinden daha tehlikeli sonuçlara yol açabilir.
- saldırıların finansal bir amacı vardır ve bu nedenle kuruluşlar önemli miktarda para kaybetmiştir.
- yazılım ve işletim sistemlerindeki güvenlik açıklarından çok insan hatasına dayandığından özellikle tehlikelidir.

Şirketler :

- üretkenlik kaybı, çalışanların moralinde düşüş ve toparlanma güçlüğü yaşayabilirler.
- müşteriler kuruluşun kendisini koruyabileceğine ikna olmadıkları için itibar zedelenmesi yaşarlar.
- genellikle eski bir olay yanıtını tetikleme ihtiyacı duyar.
- gelecekteki saldırıları önlemeye yardımcı olacak güvenlik yazılımı sağlamalıdır.
- genellikle saldırılara hazır olmaları için çalışanları yeniden eğitmek zorunda kalırlardı.

Sosyal Mühendislik Eğitimi (siber farkındalık)

- kurban olma riski yüksek olduğu için sosyal mühendislik saldırılarını tanımanın önemli olduğu çalışanlar ve yöneticiler .

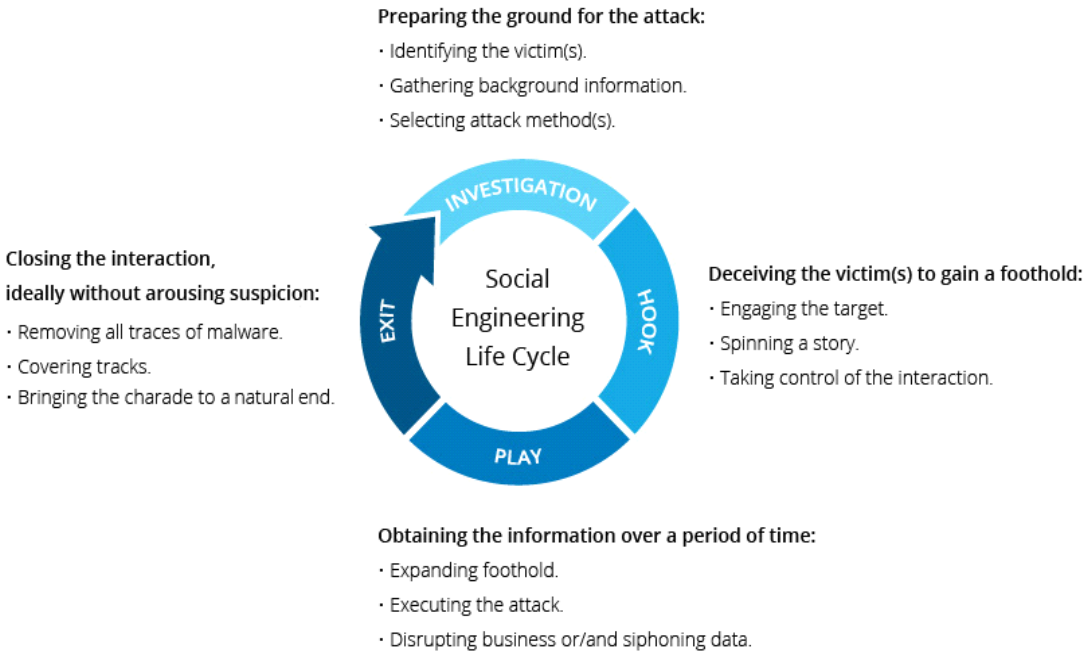
- topluluk, birey ve yurttaş güvenlik farkındalığı programlarına dahil edilebilir ve bireyleri ve kuruluşlarını koruyabilir.
- özellikle daha az kaynağa sahip olan KOBİ'lerde eksiktir, bu nedenle siber bilinçlendirme eğitimlerini ciddiye almaları ve çalışanlara bu eğitimi almaları için fırsatlar sağlamaları için onlara yardım edilmelidir.

Sosyal Mühendislik Saldırısı Yaşam Döngüsü

Saldırgan:

- saldırı için gerekli olan giriş noktaları ve zayıf güvenlik protokolleri gibi gerekli temel bilgileri toplamak için önce hedeflenen kurbanı araştırın.
- sonra deneyin, kurbanın güvenini kazanın ve hassas bilgiler haline gelme veya kritik kaynaklara erişim izni verme gibi genellikle güvenlik uygulamaları olmayan eylemler için teşvikler sağlayın.

Şekil 2, bir saldırının yaşam döngüsünü açıklar.



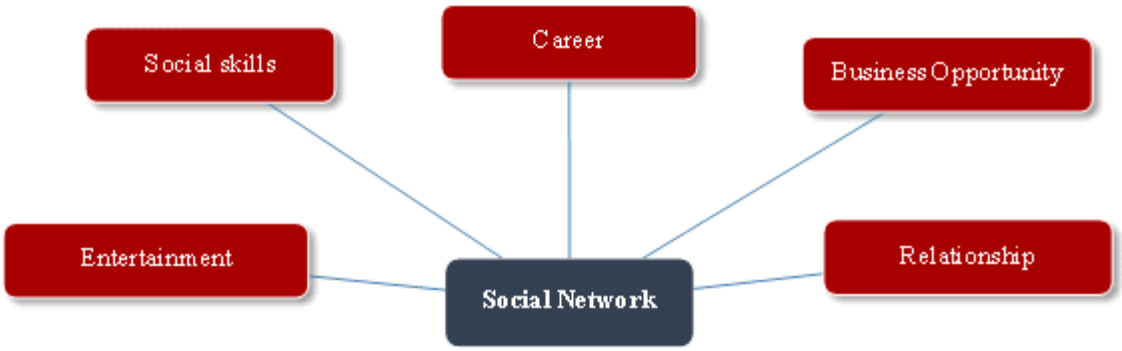
Şekil 2: Bir saldırının yaşam döngüsü

Sosyal ağ

- kullanıcılara aileleri, arkadaşları ve meslektaşları ile iletişim kurmaları için bir platform sağlayarak son yıllarda oldukça popüler hale geldi.
- ve Sosyal Ağ, arkadaşlar, aile, meslektaşlar, müşteriler veya müşterilerle bağlantı kurmak ve onlarla iletişim kurmak için İnternet tabanlı sosyal ağ sitelerinin kullanımını ifade eder.
- sunucuları, İnternet'in ana ağ erişim noktalarıyla aynı yerde bulunan veri merkezlerinde bulunur.

Sosyal Medya Rolleri (Şekil 3), sosyal medyanın rol oynadığı bazı alanları gösterir:

- Eğlence
- iş fırsatları oluşturmak
- bir kariyer yapmak için
- sosyal becerileri geliştirmek
- diğer bireylerle ilişkiler geliştirmek



Şekil 3: Sosyal Ağdaki Roller

Sosyal ağ :

- marka bilinirliğini artırmak, marka sadakatini artırmak, dönüşüm oranlarını iyileştirmek, yeni, yeni ve eski müşterilere erişim ve katılım sağlamak için müşteri arayan pazarlamacılar için bir temeldir.
- sosyal ağlarda blog yazıları, resimler, videolar veya yorumlar paylaşarak daha fazla kişinin şirketin web sitesini ziyaret etmesini ve müşteri olmasını sağlamak.
- hem değişimlere ayak uydurmayı zorlaştırır hem de bir şirketin pazarlama başarı oranını etkiler.

Amerika Birleşik Devletleri ve Avrupa'daki en popüler sosyal ağ (sosyal medya) siteleri şunlardır:

- Facebook

- Instagram
- Twitter
- Youtube
- Profesyonellerin iş arkadaşları, iş bağlantıları ve işverenlerle bağlantı kurmasına yardımcı olan LinkedIn.

insanların ve işletmelerin birbirleriyle bağlantı kurmasına, ilişkiler geliştirmesine, bilgi, fikir ve mesaj paylaşmasına olanak tanıyan teknoloji ve sosyal ağ sitelerini (Sosyal Medya) kullanarak kişisel ve ticari ilişkileri geliştirmeye ve sürdürmeye dayanır .

Aile üyeleri, Facebook gibi kişisel sosyal ağlar aracılığıyla bağlantıda kalabilir, fotoğraf paylaşabilir ve hayatları hakkında başka mesajlar gönderebilir.

İnsanlar ayrıca aynı ilgi alanlarını paylaşan başkalarıyla (yabancılarla) bağlantı kurabilir.

Yanlış bilgilerin yayılması ve sosyal medya profillerini kullanmanın ve sürdürmenin yüksek maliyeti dahil olmak üzere sosyal medyanın dezavantajları da vardır.

Sosyal platformların işlevselliği şu şekilde sınıflandırılabilir:

Ağ işlevleri, sanal platformlar içindeki kullanıcılar arasındaki sosyal ilişkileri güçlendirmeye hizmet eder ve sosyal ağ grafiğini oluşturmak ve sürdürmek için işlevsellik sağlar.

Veri işlevleri, kullanıcı tarafından sağlanan içeriğin ve kullanıcılar arasındaki iletişimin yönetilmesinden, kullanıcı etkileşiminin geliştirilmesine (genişletilmesine) ve platformun daha çekici hale getirilmesine yardımcı olmaktan sorumludur.

Erişim kontrol özellikleri, kullanıcı tanımlı gizlilik önlemleri uygulamayı ve kullanıcı tarafından sağlanan veri ve bilgilere yetkisiz erişimi kısıtlamayı amaçlar.

Sosyal ağların avantajları ve dezavantajları

Faydalar

Sosyal medya, işletmelerin şunları yapmasına olanak tanır:

- Yeni ve mevcut müşterilerle bağlantı kurmak için.
- marka bilinirliği yaratabilme, tanıtabilme ve artırabilme.
- marka satışlarını ve daha yüksek arama motoru sıralamalarını artırmak için önemli olan müşterileri tarafından yapılan incelemelere ve yorumlara güvenmek.
- yeni bir marka kurabilmek. müşterilerine yüksek düzeyde hizmet göstermek.
- ürünleri ve tüketicilerle ilişkileri geliştirebilmek.

dezavantaj

- yanlış bilgilerin yayılmasına katkıda bulunabilirler.
- Bir markaya yönelik eleştiri sosyal medyada çok hızlı yayıldığı için şirketler üzerinde olumsuz bir etkisi olabilir.
- bir şirket profili oluşturmak ve sürdürmek için her hafta çalışma saatleri ve maliyet gerektirir.

Sosyal ağlarda güvenlik ve gizlilik

- Sosyal ağlarda ve medyada paylaşılan bilgiler çok hızlı yayılıyor ve bu da saldırganların bu bilgileri ele geçirmesini cazip hale getiriyor.
- Bir kullanıcı fotoğraf, video ve ses gibi kişisel içerikler yüklediğinde, kullanıcı tarafından paylaşılan bilgilerle ilgili güvenlik ve gizlilik sorunlarına saygı gösterilmelidir çünkü saldırgan, paylaşılan bilgileri gayri meşru amaçlarla kötü amaçlarla kullanabilir.
- Güvenlik ve mahremiyet konusunda kullanıcı farkındalığının olmaması, sosyal medya aracılığıyla çeşitli siber saldırılara yol açma potansiyeline sahiptir.

Tehditler üç kategoriye ayrılabilir:

- Geleneksel tehditler, kullanıcıların sosyal ağın başlangıcından beri karşılaştığı tehditleri içerir.
- Modern tehditler, kullanıcı hesaplarını tehlikeye atmak için gelişmiş teknikler kullanan saldırılardır.
- Hedefli saldırılar, belirli bir kullanıcıyı hedef alan ve herhangi bir kullanıcı tarafından çeşitli kişisel kan davaları için gerçekleştirilebilen saldırılardır.

Sosyal ağ operatörleri için çözümler

- CAPTCHA, çok faktörlü kimlik doğrulama ve arkadaşların fotoğraflı kimlik doğrulaması gibi kimlik doğrulama prosedürleri önerilmiştir.
- Müşterinin kişisel bilgileri yabancılar veya uygulamalar tarafından istenmeyen erişimden girmesine izin veren güvenlik ve gizlilik ayarı.

Kullanıcı, kendi ağlarındaki herhangi bir kullanıcı tarafından yapılan herhangi bir kötüye kullanım veya politika ihlali bildiriminde bulunur. yani, Facebook bir kullanıcı raporu aldığında, Facebook'un topluluk standartlarına göre incelenir ve kaldırılır.

Sorular :

Sorular Tartışma Forumu kısa bir açıklama ile cevaplanacak. Cevaplar, mentorluk oturumları sırasında mentor ile tartışılacaktır.

1. InCyT projesiyle ilgili beklentileriniz nelerdir?
2. Siber saldırılara karşı kendinizi nasıl korursunuz?
3. Toplum mühendisliği nedir?
4. Sosyal Ağ (Sosyal Medya)

Öz değerlendirme soruları. Öğrenci yanıtladıktan sonra sonuçları görebilir ve bunları platformda kayıtlı sonuçlarla karşılaştırabilir.

- Siber saldırılara karşı kendinizi nasıl korursunuz?
- Toplum mühendisliği nedir ?
- Sosyal Ağ (Sosyal Medya)

Ekler

Powerpoint sunum
Video filmler

Referanslar:

- InCyT – Disiplinlerarası Siber Eğitim
- Siber Olay Kurtarma
- Siber Saldırıları En Aza İndirin - Siber Direnç Stratejisi
- Siber Saldırılar Nasıl Önlenir: Kendinizi Korumanın En İyi Yolları
- Sosyal Medya Güvenliği: Bilgileriniz Ne Kadar Güvende?
- Bilgi Sistemleri Üzerindeki İç Kontroller
- Sosyal Medya Benimseme Yeni Riskler Getiriyor
- Sosyal Medya Güvenliği – 5 Güvenlik İpucu
- 19 Sosyal Medya Güvenliği En İyi Uygulamaları