

Bilgi güvenliği bilincinin genele yayılması

Fatih Emiral

Deloitte

İnsan faktörü bilgi güvenliği programlarındaki en zayıf halka olarak nitelendirilmektedir. Kullanıcılar kasıtlı veya kasıtsız olarak, bilgi ağı ve kurumları tehditlere açık halde bırakmaktadır. Güvenlik programları çoğunlukla insan faktörü yerine, teknik kontrollere odaklanma eğilimindedir.

İnsana bağlı güvenlik riski hiçbir zaman tamamen yok edilemese de iyi planlanmış bir kullanıcı bilinçlendirme çalışması, riskin kabul edilebilir bir seviyeye indirilmesine yardımcı olacaktır. Kullanıcıların bilgiyi ve bilgi kaynaklarını koruma konusunda üzerlerine düşen sorumlulukları anlaması kritik öneme sahiptir. Burada bilgi güvenliği bilincinin önemi ve bir bilgi güvenliği programının temel hedeflerini nasıl desteklediği anlatılmaktadır. Bunun yanı sıra etkili bir bilinçlendirme stratejisinin nasıl uygulanabileceği konusunda öneriler sunulmaktadır. Uygulamalarda karşılaşılmış engel ve zorluklar da aşağıda belirtilmektedir.

Bilgi güvenliği bilinçlendirme çalışmasının hedefleri

Bilinçlendirme programının temel hedefi, kullanıcıları kurumsal bilgi ve bilgi kaynaklarının gizlilik, bütünlük ve devamlılığı konusundaki görev ve sorumlulukları konusunda eğitmektir. Bilgi güvenliği sadece Bilgi Teknolojileri güvenlik ekibinin değil, tüm personelin sorumluluğudur. Kullanıcılar sadece bilginin korunması konusunda nasıl katkı sağlayabileceklerini değil, aynı zamanda bilginin neden korunması gerektiğini de öğrenmelidir. Kullanıcılar ya eğitimsizlikten ya da güvenlik hakkındaki bilinç eksikliğinden, genellikle güvenlik zincirinin en zayıf halkası olarak değerlendirilmektedir. Çalışanlar, hatalı davranışlarının kurum bilgi güvenliği üzerinde yaratabileceği etkiyi anlamalıdır. Kullanıcı bilinçlendirme çalışmaları, güvenlik ihlallerinin maliyetini azaltmaya ve kontrollerin kurumun tüm bilgi kaynakları üzerinde dengeli uygulanmasına yardımcı olacaktır.

Güvenlik bilinçlendirme çalışmaları genellikle iki farklı, ancak ilişkili parçaya ayrılır; bilinçlendirme ve eğitim. Bilinçlendirmenin amacı, güvenlik ve güvenlik kontrollerinin önemi hakkında kolektif bir bilinç oluşturulmasıdır. Bilinçlendirme mesajları basit ve açık olmalı, sunumu hedef kitlesinin kolayca anlayabileceği bir formatta yapılmalıdır. Eğitimin amacı ise kullanıcı anlayışının derinleştirilmesidir. Eğitim yöntemleri, sınıf dersleri, bire bir eğitim veya eğitim paketleri olabilir.

Başarıya ulaşma konusunda karşılaşılabilecek engeller

Ne yazık ki, başarılı bir bilinçlendirme çalışması uygulanması zor ve başarılması imkansız görev olarak görülebilir. En iyi planlanmış programlar dahi birtakım engeller ile karşılaşabilir. Bu nedenle bir program uygulamadan önce, karşılaşılabilecek engellerin anlaşılması faydalı olacaktır.

Eski köye yeni adet

Pek çok organizasyonda güvenlik fonksiyonlari ihtiyacının gölgesinde kalmakta ve uygulanmasında geç kalınmaktadır. Güvenlik uygulamaları başından itibaren uygulanmadığından, kullanıcılar kötü alışkanlıklar edinmek için aylar, hatta yıllara sahiptir. Bu durum bilgi güvenliği bilinçlendirme programının uygulanmasını iki kat zorlaştırır. Çünkü sadece kullanıcıları eğitmek değil, aynı zamanda eski alışkanlıklarından kurtarmak gerekmektedir. Bunun yanında kullanıcılar da bilinçlendirme programını kabul etmek için fazladan sorun yaşar. Kullanıcılara göre kurum, güvenlik önlemleri olmaksızın gayet iyi çalışmıştır. Yeni güvenlik önlemleri hayatı zorlaştırıcı gereksiz değişiklikler olarak görülür.

Güvenlik, bilgi teknolojilerinin problemi, benim değil

Çoğu kullanıcı, bilgi güvenliğinin Bilgi Teknolojileri Güvenlik Bölümü'nün sorumluluğu olduğu, kendilerini ilgilendirmedeği fikrine sahiptir. Rollerini işlerinin gerektirdiği minimum uyumu göstermekle sınırlı görüp, kuruma faydalı olabilecekleri büyük resimdeki yerlerini göz ardı etme eğilimindedirler. Politika ve prosedürlere uyum iyi bir başlangıç olmakla birlikte, daha yapılacak çok fazla iş vardır. Kullanıcıların Bilgi Teknolojileri Bölümü'nün bu işi tek başına yapamayacağını anlaması gerekir.

Yeni teknoloji

Yeni teknolojinin kuruma katılması, genellikle kullanıcı davranışlarının değişmesi veya yeni bir bakış açısına sahip olmasını gerektirir. Bu bir sorun teşkil etmemektedir, ancak, teknoloji bazen bilinçlendirme programından hızlı veya bağımsız olarak ilerlemektedir. Çoğu zaman bilinçlendirme ekibi sürecin dışında veya eğitim gereksinimleri konusunda zamanında bilgilendirilmemiş olmaktadır. Bu nedenle bilinçlendirme programı, bölümler arası iletişim, acil durum ve kriz iletişimi konuları üzerinde durmalıdır.

Tek ölçü farklı beden

Bazı bilinçlendirme programları hedef kitesini doğru sınıflandıramamakta ve hedef kitleye uygun mesajları iletememektedirler. Bu hatalı strateji, iletilen mesajların kulak ardı edilmesine neden olmaktadır. Kullanıcılar gündelik hayatlarında etraflarından yüzlerce mesaj almaktadır. Kullanıcıların sınıflandırılması ve sadece ihtiyaç duydukları mesajları almaları son derece önemlidir. Her bedene tek ölçü stratejisi, programı uygulayanlar açısından kolay olabilir, ancak etkili olmayacaktır.

Aşırı bilgi

Bir diğer hata da fazla eğitimidir. İnsanlar herhangi bir kaynaktan gelebilecek bilgiye karşı bir eşik değerine sahiptirler. Bir kişi sürekli olarak mesaj verilmeye zorlanırsa, bir süre sonra eşik değeri aşılabileceği ve ilgisi kaybolacaktır. Doğru sınıflandırma yapılsa bile, fazla bilgi fazla bilgidir. Bilinçlendirme programı bir akşamda bitirilmek zorunda değildir. Hedef kitleden gelen tepkiler dinlenmeli ve denge kurulmalıdır.

Organizasyon bozukluğu

Pek çok bilinçlendirme çalışması, tutarlı ve düzenli bir strateji ile mesajlarını hedef kitesine ulaştıramamaktadır. Tutarlı ve düzenli bir çerçeve olmadan kullanıcıların programı benimsemesi ve hatta ne amaçla yapıldığını algılaması bile zorlaşacaktır. İletişimde tutarlılık ve düzenin sağlanması programa kişilik kazandıracaktır.

Takip etmeme

Bilinçlendirme programlarının bir başlangıç heyecanı ile başlatılması, ancak çok az başarı sağlaması olağandır. Pek çok program düzenli ve periyodik olarak gerçekleşen bir iletişim çemberini kuramamaktadır. Kullanıcılar ile düzenli iletişimin sürdürülmesi, anahtar mesajları hatırlamaları açısından önemlidir. Bunun yanında pek çok program hedef kitesinin düşüncelerini öğrenmeyi ihmal eder. Hedef kitlenin dinlenilmesi ve programın onların ihtiyaçlarına uygun biçimde düzenlenmesi çok önemlidir.

Yönetim desteğinin bulunmaması

Yönetim desteği, bilgi güvenliği kullanıcı bilinçlendirme programının olmazsa olmaz unsurudur. Güvenlik mesajlarının etkili olabilmeleri için en yukarıdan desteklenmeleri gereklidir. Pek çok yönetici bu tür çalışmalar konusunda desteğini dile getirirse de, desteğin gerçekleşmesi söylemek kadar kolay olmamaktadır. Bu durum yöneticilerin kendi iş ve sorumluluklarının bulunmasından kaynaklanmaktadır. Yönetimin temel hedefi iş hedeflerine ulaşmak olup, güvenliğin önemine ne kadar inansalar da zaman ayırmaları güç olmaktadır.

Kaynak eksikliği

Bu durum genellikle yönetim desteğinin eksikliğinden kaynaklanmaktadır. Yönetim desteği olmaksızın gerekli kaynağı ayırmak çoğu zaman imkansızdır, kaynak eksikliği de böyle bir durumda nasıl bir sonuç elde edilebilir ise ona ulaşmaya mahkumdur.

"Neden" sorusunun yanıtlanmaması

Pek çok bilinçlendirme programı kullanıcıları bilgi güvenliğinin neden önemli olduğu konusunda eğitmeyi başaramamaktadır. Bu programlar diğer tüm konuları kapsamakta, ancak kullanıcı motivasyonunu artıracak en önemli konuyu atlamaktadır. Bazı davranışların neden güvenliği zayıflattığını anlayan kullanıcılar, bilgi güvenliğine sahip çıkıp, davranışlarını değiştireceklerdir. Örneğin, daha sıkı kurallara sahip bir şifre politikasını kullanıcılara iletirseniz, onlar bu politikayı bir yük olarak görecektirler. Diğer taraftan kullanıcılara şifrelerin nasıl kırıldığını ve kötü niyetli kullanılabilirliğini, bu durumun potansiyel sonuçlarını anlatırsanız, kullanıcılar politikaya sahip çıkarak, yeni politikayı uygulamaya gönüllü olacaklardır.

Sosyal mühendislik

Sosyal mühendislik bilinçlendirme programının uygulanmasını etkilemez, ancak başarısını etkileyebilir. Bu konuya önem verilmesi, güçlendirmeye çalıştığımız insan faktörünü hedef alması açısından önemlidir. Sosyal mühendislik, insan doğasında var olan başkalarına güvenme ve yardım etme eğiliminin başka şekilde elde edilmesi zor olan şeylerin ele geçirilmesi amacı ile kullanılmasıdır. İnsanlar başkalarının maksatlı olarak kendilerini tuzağa düşürmeyecekleri veya kullanmayacaklarını düşünme eğiliminde olsalar da bu yöntem en sık kullanılan saldırı yöntemlerindedir. Bu yöntem öyle kolay ve hızlıdır ki, saldırganlar sık sık bu yöntemle başvururlar. Öyle ya, bir saldırgan yardım masasından arıyormuş gibi davranarak kolayca şifrenizi almak varken, neden saatlerce şifrenizi kırmaya çalışsın. En yaygın sosyal mühendislik yöntemleri; başka birisiymiş gibi davranma, kompliman, aciliyet ve otorizasyon alınmış duygusu yaratmadır. Bu nedenlerle kullanıcıların sosyal mühendisliğe karşı korunmasını hedefleyen bir eğitim stratejisi izlenmelidir.

Etkili bir bilgi güvenliği bilinçlendirme programının geliştirilmesi

Etkili bir bilgi güvenliği bilinçlendirme programının geliştirilebilmesi için aşağıdaki adımlar izlenebilir:

Bilgi güvenliği politikasının geliştirilmesi

Güçlü ve anlamlı bir bilgi güvenliği politikası, her başarılı bilinçlendirme çalışmasının temelini oluşturur. Bilinçlendirme çalışmasına başlamadan önce, tüm üst seviye hedeflerin ve güvenlik programının gereklerinin dokümanite edilmiş olması kritik önem taşımaktadır. Politika açık ve kısa ifadeler ile yazılmış olmalı ve kurumun bilgi güvenliği konusundaki önceliklerini yansıtmalıdır. Politika ortaya konduktan sonra, kullanıcılar politikanın varlık ve içeriğinden haberdar olmalıdır. Kullanıcılar aynı zamanda politikaya uymamanın doğuracağı sonuçlar hakkında da bilgi sahibi olmalıdır.

Mevcut eğitim ihtiyaçlarının belirlenmesi

Başarılı bir bilinçlendirme programının geliştirilmesindeki ikinci adım, kurum personelinin mevcut eğitim ihtiyaçlarının belirlenmesidir. Bu adım genellikle göz ardı edilmekte veya geçiştirilmektedir. Pek çok durumda programlar kullanıcı ihtiyaçlarının dinlenmesi yerine, varsayımlara dayanılarak geliştirilmektedir. Kullanıcıların güvenlik konusundaki mevcut bilgi düzeyinin ölçülmesine zaman ayrılması eğitim ihtiyaç ve önceliklerinin doğru tespitine yardımcı olacaktır. Aşağıdaki maddeler bu adımda ortaya çıkarılabilecek konuları içermektedir:

- Kullanıcıların öğrenme stil ve tercihleri
- Özel ilgi veya endişe alanları
- Bilinçlendirme programına karşı duyulan direnç ya da sempati
- Daha önceki başarılı veya başarısız eğitim girişimleri
- Daha önceden mevcut bulunan eğitim kaynak ve materyalleri
- Programın başarısı için destek alınabilecek kişi veya grupların tespiti

Ön araştırmanın yapılması ile mevcut kaynakları en iyi biçimde kullanıp, başarı şansını yükselten bir bilinçlendirme programı tasarlanması mümkün olabilir. Aşağıda mevcut eğitim ihtiyaçlarının tespitinde kullanılabilecek bazı yöntemler bulunmaktadır:

- Farklı kıdem, unvan ve iş tanımlarına sahip kullanıcılar ile görüşme
- Genel kullanıcılara temel güvenlik bilgileri hakkında anket veya kısa soru listesi gönderme

- Kurumda son zamanlarda karşılaşılmış güvenlik problemlerinin tespiti (örneğin geçen yıl çalınan diz üstü bilgisayarların sayısı)
- Sistem, uygulama ve bilgi ağı denetimlerinin gerçekleştirilmesi
- Farklı birimlerle yüz yüze toplantılar gerçekleştirilmesi
- Bina ve kullanım alanlarının ziyaret edilmesi ve mevcut fiziksel güvenlik seviyesinin gözlenmesi. Kilitlenmemiş ofis odaları, dolaplar ve güvenliği bulunmayan kişisel bilgisayar ve bilgilerin izlenmesi.

Üst yönetimin desteğinin sağlanması

Güvenlik ihtiyacının tespitinden sonraki aşama, üst yönetimin ve kurum içinde otorite sahibi pozisyonlardaki kişilerin desteğini almaktır. Ne yazık ki, bir bilinçlendirme programı ihtiyacının kabul ettirilmesi zor bir iştir. Bilgi güvenliği bilinci sadece iş hedeflerine ulaşmada karşılaşılan bir engel olarak görülmez, aynı zamanda bilgi güvenliğinin göz ardı edilen bir parçası olarak kalır. Güvenlik bilinci genellikle firewall ve anti-virüs araçlarının uygulanmasının arkasında bir öneme sahip olarak kalır.

Üst yönetimin desteğinin sağlanmasında iki temel hedef akılda tutulmalıdır. Birinci hedef kaynak teminidir. Bu tür bir programı uygulamak, bazı kaynakların bu iş için kullanılmasını gerektirecektir. Kurumun büyüklüğüne göre gerekli bütçe sağlanmalıdır. İkinci, ancak daha az öneme sahip olmayan hedef güvenlik hamilerinin kurum içinde oluşmasını sağlamaktır. Sadece maddi kaynak yaratan değil, aynı zamanda davranışları ile diğer kişilerin de bilinçlendirme programına değer vermeleri ve programa katılmalarını sağlayan kişilerin bulunması, başarı için çok önemlidir. Yöneticileri eğitimin önemini ortaya koyup desteklerse, çalışanlar eğitime katılma ve yarar sağlama konusunda daha istekli olur.

Üst yönetimin desteğinin sağlanması için yönetimin bilinçlendirme çalışmasının kurumsal bilgi ve bilgi kaynaklarının korunmasındaki hayati rolünü anlamasına yardımcı olunması gerekmektedir. Ancak bu aşamaya gelindiğinde kurumun güvenlik ihtiyaç analizi yapılmış olduğundan, endüstri istatistik ve örnekleri ile de desteklenen materyaller gerekli desteğin sağlanmasında yardımcı olacaktır.

Hedef kitlelerin belirlenmesi

Bir sonraki önemli adım hedef kitlelerin belirlenmesidir. Herkes işlerini yapabilmek için aynı derece veya tipte güvenlik bilincine ihtiyaç duymaz. Kullanıcı grupları arasında gerekli ayrımı yapan ve her gruba sadece ilgili bilgiyi sunan bir bilinçlendirme programı, en iyi sonucu elde edecektir. Günümüzde her birimiz bilgi bombardımanına tutulmaktayız. İletmek istediğiniz mesajların kulak ardı edilmesini istemiyorsanız, sadece gerekli bilgiyi gerekli kitleye iletmenizdir. Tek bir programın herkes için uygun olacağı düşüncesi, programın işe yaramamasına neden olabilir.

Hedef kitleler çeşitli biçimlerde ayrıştırılabilir. En çok kullanılan bazı yöntemler aşağıdaki gibidir:

- Bilinç seviyesi
- Teknik bilgi seviyesi
- Unvan/Yetki seviyesi
- İş fonksiyonu
- Kullanılan teknoloji, sistem ya da uygulama

Kurum için istenen sonucu ürettiği sürece, hangi kriterlerin kullanıldığı önemli değildir. Büyük kurumlarda yukarıda sayılan yöntemler kombinasyon halinde 4 ana kategoriyi belirlemek için kullanılabilir. Bu kategoriler gerekiyorsa daha alt gruplara bölünebilir. 4 ana kategori aşağıda belirtildiği gibidir:

- Üst Yönetim - Kurumun stratejik hedeflerini belirleyen en üst seviyedeki yönetim kademeleri
- Yönetim - Orta seviye ve lider görevi taşıyan yöneticiler

- Teknik Kullanıcılar - Sistemler üzerinde sıra dışı erişim haklarına ve bilgiye sahip personel. Bu kullanıcılar sistem ve kullanıcı yönetimi, donanım bakımı, uygulama geliştirme ve uyarlaması ve teknik destek hizmetlerini yerine getirmektedir.
- Son Kullanıcılar - Kurumun bilgi kaynaklarını kullanmaya yetkili tüm kullanıcılar. Bu grup diğer üç grupta bulunan kullanıcıları kapsamaktadır.

Kilit mesajların belirlenmesi

Her gruba özgü kilit mesajları oluşturmadan önce tek bir çekirdek ifade veya misyon ifadesi belirlenmelidir. Bu çekirdek ifade bilgi güvenliği politikası içinde belirtilmiş olabilir, ancak bu aşamada da düşünülmelidir. Diğer tüm kilit mesajlar bu ifadeyi desteklemeli ve işaret etmelidir. Böyle bir ifadeye örnek olarak:

- Bilgi güvenliği bilinçlendirme programının misyonu kurumun bilgi ve bilgi kaynaklarının gizlilik, bütünlük ve devamlılığının korunmasıdır.

Bir sonraki adım her grup için üst seviye, kilit mesajların oluşturulmasıdır. Bunun yapılabilmesi için, kurumun bilgi güvenliği politikasındaki ifadeler hedef kitlelere göre sınıflandırılmalıdır. Bu mesajlar sadece program misyonunu desteklememeli, aynı zamanda daha detaylı mesajlar için zemin oluşturmalıdır. Aşağıdakiler hedef kitlelere göre belirlenmiş üst seviye kilit mesaj örnekleridir:

Üst yönetim

- Güvenlik süreçlerinde üst yönetim gözetim ve rehberliğini sağla
- Güvenlik yatırımlarının iş öncelikleri ile uyumunu sağla
- Kurum ve birimlere özgü güvenlik politika ve standartlarına uyumu temin et

Yönetim

- Güvenlik politika ve standartlarını anlama ve uyuma yönelik süreç ve önlemleri geliştir
- Mevcut ve yeni gelecek iş süreçlerindeki potansiyel güvenlik risklerini belirle ve önlem al

Teknik kullanıcı

- Yönetimin belirlediği politika, standart ve prosedürleri uygula
- Son kullanıcılar için gerekli prosedür ve teknik önlemleri uygulayarak güvenlik politika ve standartlarına uyumu sağla

Son kullanıcı

- Kurumun bilgi ve bilgi kaynaklarının gizlilik, bütünlük ve devamlılığını koru
- Kurumun bilgi güvenliği politika ve standartlarında belirtilen son kullanıcı sorumluluklarına uy

Her hedef kitle için üst seviye mesajlar belirlendiğinde detay mesajlar ve eğitim ihtiyaçları belirlenebilir. Bunu yapabilmek için güvenlik programının yapı taşları ve son zamanlarda gerçekleşen güvenlik ihlalleri gözden geçirilebilir. Gözden geçirilebilecek bazı yapı taşları aşağıdaki gibidir:

- Güvenlik politika, standart ve prosedürleri
- İlgili kanuni düzenlemeler
- Son olaylar (yetkisiz erişim, virüs bulaşması gibi)
- Sistem, uygulama ve bilgi ağı denetim sonuçları
- Eğitim talepleri
- Yeni teknolojinin kullanılmaya başlanması
- Birinci adımda tespit edilen bulgular (Mevcut Eğitim İhtiyaçlarının Belirlenmesi)

Ele alınabilecek bazı özel güvenlik konuları aşağıdaki gibi olabilir:

- Şifreler

- Fiziksel güvenlik - kurum içi ve dışında
- Sosyal mühendislik
- Virüsler
- e-Posta ve İnternet kullanımı
- Onaylanmamış yazılım ve donanım kullanımı
- Erişim kontrolü (en az yetki, rollerin ayırımı ve yedekleme ilkeleri)
- İş sürekliliği ve felaket kurtarma

Bu adım periyodik olarak uygulanmalı, ancak ilk olarak bilinçlendirme programının temelini oluşturacak biçimde gerçekleştirilmelidir. Yukarıdaki maddeler her zaman yeni ihtiyaçların ortaya çıkıp çıkmadığının belirlenebilmesi için değerlendirilmelidir. Güvenlik programları yeni koşullara uyum sağlayabilecek esneklikte olmalı, gerektiğinde içerik ve mesajların öncelikleri yenilenmelidir. Hedef kitleye uygun ve anlaşılabilir nitelikte mesajlar üretilmelidir. Gerçek hayat örneklerinin çalışmaya katılması programa olan ilgiyi artıracaktır.

Mevcut iletişim araçlarının belirlenmesi

Bilinçlendirme programındaki bir sonraki adım mevcut iletişim araçlarının belirlenmesidir. Her kurum kendine özgü iletişim olanaklarına sahiptir. Bu kaynakların tespiti yapılmalı, kaynakların kullanımına yönelik prosedürler anlaşılmalıdır. Örneğin bazı kurumlar kurum genelinde yapılacak yayınlar için üst yönetim onayını şart koşmaktadır. Bazı yaygın iletişim araçları aşağıdaki gibidir:

- Herkese gönderilen e-posta
- Özel kişilere gönderilen e-posta
- Herkese gönderilen sesli posta
- Şirket genelgesi
- Bölüm genelgesi
- Intranet
- Yazılı yayın - posterler, dönemsel şirket yayını, broşürler
- Yüz yüze - toplantılar, sunumlar, eğitim ve güvenlik seminerleri
- Kütüphane - videolar, kitaplar ve etkileşimli sunumlar
- Hatırlatıcı malzemeler - sisteme giriş mesajı, pazarlama araçları (kalem, silgi, mouse pad, anahtarlık, not kağıtları, vb.)

İletişim aracının seçiminde farklı kitlelerin farklı biçimlerde öğrenmeye açık oldukları düşünülmelidir. İletişimin etkili olması için birden fazla kanal kullanılabilir.

Uygulama için strateji geliştir

Başarılı bir bilinçlendirme çalışmasının uygulanabilmesi için gerekli son adım, mesajların tutarlı ve etkili iletimi için bir çerçeve geliştirilmesidir. Bu çerçeve geliştirilmeden iletilen mesajlar kullanıcılar tarafından düzensiz ve gelişmiş güzel bir çalışmanın eseri olarak algılanacaktır. Uygun stratejinin geliştirilebilmesi için, hedef kitleler, kilit mesajlar ve iletişim imkanları göz önüne alınmalı, programın tekrarlanabilir bir süreç haline getirilmesi sağlanmalıdır.

Bu adımın bir parçası olarak, açık bir pazarlama stratejisi belirlenmelidir. Pazarlama araçları şunları içerebilir: Logo, slogan, ofis araçları.

Bilinçlendirme stratejisi

Bilinçlendirmenin amacı temel olarak kullanıcıların bilgi ve bilgi kaynaklarının korunma ihtiyacını anlamasıdır. Aşağıdakiler, bilinçlendirme stratejisinin parçası olarak tekrarlanabilir taktiklerdir:

- İşe alım sırasında yapılacak bilgilendirme
- Aylık şirket bülteni
- Şirket yemek ve eğitimleri

- Yıllık güvenlik seminerleri
- Bilgi güvenliği konusundaki başarılar için teşvik ödülleri
- Oyunlar, yap-bozlar ve yarışmalar

Eğitim stratejisi

Eğitim ve öğretimin amacı, kullanıcıların bilgi güvenliği, bilgi ve anlayış seviyelerinin artırılmasıdır. Aşağıdakiler, eğitim ve öğretim stratejisinin parçası olarak tekrarlanabilir taktiklerdir:

- Temel son kullanıcı eğitimi
- Teknik eğitim
- Gelişmiş bilgi güvenliği eğitimi - Bu eğitim bilgi güvenliği uzmanları ve denetçileri içindir
- Dönemsel eğitim paketi - Bu araç her dönem özel bir bilgi güvenliği konusuna odaklanmalıdır. Bu eğitimler bilinçlendirme paketinden daha derin bilgi vermeyi hedeflemelidir.

Ölçebilme kabiliyeti

Ölçüm bilinçlendirme programının son adımıdır. Programın ilk uygulamasında belli bir kullanıcı bilinç seviye taban değerinin oluşturulması önemlidir. Çünkü bu seviyede ileride meydana gelebilecek gelişme veya gerilemeler ölçülebilir. Mevcut durum değerlendirmeleri yeni bir program ve strateji uygulanmadan önce de yapılmalıdır. Eğitim ve bilinç seviyesinin ölçümü kolay olmadığından, yaratıcı olunmasını gerektirir. Somut bazı ölçütlere ulaşılabilir, ancak çoğunlukla kalitatif ölçütlere dayanılması gerekmektedir.

Sonuç

Bilgi güvenliğinin önemi gün geçtikçe artmakta ve bilgi güvenliği daha karmaşık bir hal almaktadır. Yeni açık ve virüsler her gün ortaya çıkmaktadır. Teknoloji seviyesi ve saldırılardaki artışlarla, kullanıcıların bilinç ve eğitim seviyelerindeki yetersizlik açığa çıkmaktadır. Pek çok kullanıcı bilgi ve bilgi kaynaklarının korunmasının önemi konusunda ya çok az anlayışa sahiptirler ya da hiç bir anlayışa sahip değildirler. Kurumlar açısından, uygulanacak bir bilgi güvenliği bilinçlendirme çalışmasının önemini anlamaları ve eğitim eksikliğinin giderilmesi kritik öneme sahiptir. İyi tasarlanmış ve yürütülmüş bir bilinçlendirme çalışması, güvenlik zincirinin en kırılgan halkasının güçlendirilmesinde büyük etki yaratacaktır.

FATİH EMİRAL

Deloitte Kurumsal Risk Hizmetleri

MAYIS 2004, ACTIVELINE