1. AMAÇ

Bu prosedür, S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi bünyesinde görev yapan tüm kamu çalışanlarının, sözleşmeli çalışanların ve Müdürlük internet ağı, bilgi sistemlerine erişim sağlayan tüm kullanıcıların, kurumsal bilgilerin sosyal mühendislik saldırıları ile ele geçirilmesini önlemek ve sosyal medya kullanımı nedeniyle doğacak kurumsal bilgi güvenliği ihlalleri ile sosyal mühendislik zafiyetlerini önlemek amacıyla uyması gereken S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi prosedürünü tanımlamaktadır.

2. KAPSAM

Bu prosedür S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi bünyesinde görev yapan tüm kamu çalışanlarının, sözleşmeli çalışanların ve Müdürlük internet ağı, bilgi sistemlerine erişim sağlayan tüm kullanıcıların herhangi bir ortamda (telefon, e-posta, sohbet vb.) 3. şahıslarla yapacakları kurumsal veri paylaşımı süreçleri ile sosyal medya araçlarını kullanım süreçlerini kapsamaktadır.

UYGULAMA

Sosyal mühendislik temel olarak insan ilişkilerini veya insanların dikkatsizliklerini kullanarak hedef kişi ya da kurum hakkında bilgi toplamak olarak tanımlanabilir. Bu olayda amaç hedef kurum veya kişi yapısı, kurumsal ağın yapısı, çalışanların/yöneticilerin kişisel bilgileri, şifreler ve saldırıda kullanılabilecek her türlü materyalin toplanmasıdır.

Sosyal Medya ise tek yönlü bilgi paylaşımından, çift taraflı ve eş zamanlı bilgi paylaşımına ulaşılmasını sağlayan medya sistemidir. Ayrıca sosyal medya; kişilerin internet üzerinde birbirleriyle yaptığı diyaloglar ve paylaşımların bütünüdür.

Kurumsal bilgilerin sosyal mühendislik saldırıları yoluyla yetkisiz kişilerin eline geçmemesi ve sosyal medya kullanımı süresince oluşabilecek bilgi güvenliği ihlallerinin önlenmesi için tüm kullanıcıların aşağıda belirtilen kurallara uymaları gerekmektedir.

2.1. Sosyal Mühendislik Zafiyetleri

2.1.1. Her kullanıcı görevi gereği yaptığı iş ve işlemler ile eriştiği, işlediği ve taşıdığı tüm kurumsal verilerin sadece kuruma ait önemli veriler olduğunun bilincinde olmalıdır.

2.1.2. Kurumsal verilerin herhangi bir ortamda paylaşımı esnasında bu verilerin yetkisiz ve kötü niyetli şahıslarca ele geçirilmesi durumunda bilgi güvenliği ve kurum açısından son derece büyük risklerin ve zararların oluşabileceği düşünülerek hareket edilmelidir.

2.1.3. Telefon, e-posta ve sohbet yoluyla yapılan paylaşımlarda kesinlikle şifre gibi özel bilgiler sistem yöneticisi dahil hiç kimseyle paylaşılmamalıdır.

2.1.4. Bir kuruma yönelik sosyal mühendislik saldırılarının tipik hedefleri, saldırganın suiistimal edebileceği durumdaki personeldir. Saldırılan profilleri aşağıdaki şekilde özetlenmiş olup sosyal mühendislik zafiyetleri açısından bu hususlar göz önünde bulundurulmalıdır.

Direkt ulaşılabilir personel (Servis elemanları, telefonlara yanıt veren çalışanlar): Kurumun dış yüzü olarak tanımlanabilecek, işi gereği müşteriler ve sağlayıcılarla iletişim kuran çalışanlar.
Önemli personel (Yöneticiler, gizli bilgiye erişim hakkı olan personel): Kurumdaki görevleri gereği zorunlu olarak ayrıcalıklı yetkiye sahip olan ya/ya da gizli bilgiye çeşitli nedenlerle erişim hakkı olan çalışanlar.
Sempati sahibi personel: Kurum içinde görevli olan, müşterilerine yardım ve destek için yetkisinden fazlasını ya da kurum içindeki itibarını kullanabilecek çalışanlar.
Destek ihtiyacındaki son kullanıcılar: Kurumun hizmetlerinden yararlandıklarından dolayı sistemlere erişimi bulunan fakat kurum hakkındaki bilgileri eksik olduğundan dolayı sistemlerle ilgili destek almaları gerektiğinde meşru destek personeliyle kötü niyetli saldırganı ayırt edemeyebilecek kullanıcılar.
Kandırılmış, aldatılmış ya da ikna edilmiş personel: Kurum içinde görevli olan ve kuruma ya da kurum çalışanlarına bağlılığı zayıflamış çalışanlar.

2.1.5. Saldıran profili ise, hedefe ve yönteme bağlı olarak değişebilir. Sosyal mühendislik saldırılarında kullanılagelen yöntemlerin bazıları aşağıda sıralanmış olup her kullanıcı bu hususlara dikkat etmelidir.

Otoriter yaklaşım: Yetkili, üst düzey yönetici ya da ayrıcalıklı müşteri olduğuna ikna etmek. **Yardım önermek:** Destek ihtiyacındaki müşteri ya da çalışanları yetkili personel olduğuna inandırmak.
Benzerlik ve ortak noktalar bulmak: Çalışanla arasında çeşitli sanal sosyal bağlantılar (akrabalık, ortak meslek, ortak arkadaş, aynı çevre v.s.) oluşturmak.
Mukabele etmek: İstenen bir iyilik için bir karşılık önermek.
Bağlılık ve dürüstlüğü suiistimal etmek: Kuruma bağlı çalışanı, saldıranın isteğini yapmaması durumunda kurumun zarar göreceğine ikna etmek.
Düşük bağlılıktan yararlanmak: Kuruma bağlılığı zayıf çalışanları ikna, aldatma ya da kandırma gibi yöntemlerle ayartmak.

2.1.6. Sürekli ve güncel eğitim ve bilgilendirme çalışmaları ile çalışanlar sosyal mühendislik konusunda bilgilendirilmeli ve bilinçlendirilmelidir.

3.1.7. Üst yönetim verilen eğitimlerin ve uyarıların izlendiğinden emin olmalı, güvenlik yönergelerine uyulmaması durumunda yaptırım uygulamaya kararlı olmalıdır.

3.1.8. Her kullanıcı bir sosyal mühendislik saldırısının tespit edildiği durumda "Bilgi Güvenliği İhlali Bildirim Formu" nu kullanarak Bilgi Güvenliği Yetkililerine haber vermekle yükümlüdür.

Hazırlayan	Kontrol Eden	Onaylayan

3.1.9. Hiç bir sistem insandan bağımsız değildir. Bilgisayar sistemleri, insanlar tarafından tasarlanır, bakımı ve işletimi insanlar tarafından yapılır ve sistemden faydalanan ve sistemi kullananlar da insandır. İnsan bileşeni aynı zamanda bir güvenlik sisteminin en zayıf halkasıdır. Bundan dolayı insan faktörünün istismarına dayanan sosyal mühendislik saldırılarının gerçekleşme olasılığının her zaman olduğu ve göz ardı edilemeyeceği açıktır. Sosyal mühendislik saldırılarının başarısı, bilgisayar ve ağ sistemlerindeki yerel zayıflıkların varlığına bağlı olduğundan, yerel açıklıklara verilmesi gereken önemi artırmaktadır. Sosyal mühendislik saldırılarının etkisini en aza indirgemenin yolu güvenlik politikalarının güncel tutulmasından ve personelin uygun bir şekilde bilgilendirilmesinden geçer. Bu nedenle Müdürlük\Birim içerisinde yapılan hizmet içi eğitim planlarında bu konuya geniş yer verilmelidir.

2.2. Sosyal Medya Güvenliği

2.2.1. Hangi sosyal paylaşım sitesinde olursa olsun, resmi olmayan hiçbir sayfa ve profile itibar edilmemesi gerekir.

2.2.2. Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.

2.2.3. Kurumsal e-posta hesapları kullanılırken, bilinmeyen adreslerden ya da kişilerden gelen e-mailler, gönderi, davet ve çağrıların açılmaması gerekir. Çünkü bunlar kurumsal\kişisel verilere ulaşmak amacı ile tasarlanmış özel maillerdir.

2.2.4. Sosyal medya araçları üzerinden yapılan paylaşımların ne olduğuna, suç unsuru taşıyıp taşımamasına mutlaka dikkat edilmelidir.

2.2.5. Aynı şekilde gelen paylaşımların da suç unsuru taşıyıp taşımamasına, küfür, hakaret, sövme, aşağılayıcı sözler içerip içermemesine dikkat edilmelidir.

3. YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla **BGYS Disiplin Prosedürü** Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır. Ayrıca gerekli görülmesi halinde sosyal medya araçları üzerinden yapılan paylaşımlar nedeniyle Kurumun suç duyurusunda bulunma hakkı mevcut

Hazırlayan	Kontrol Eden	Onaylayan