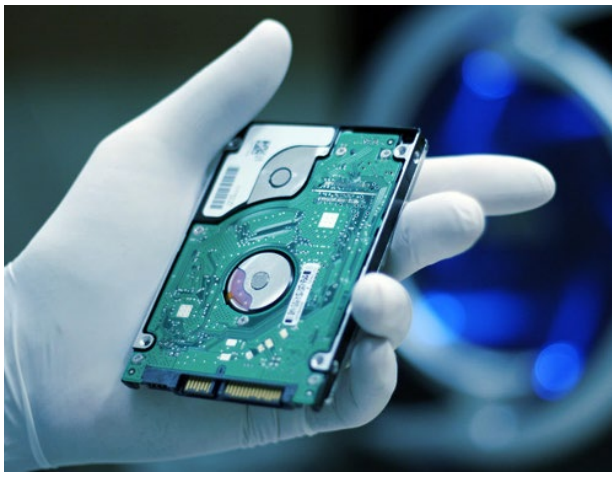
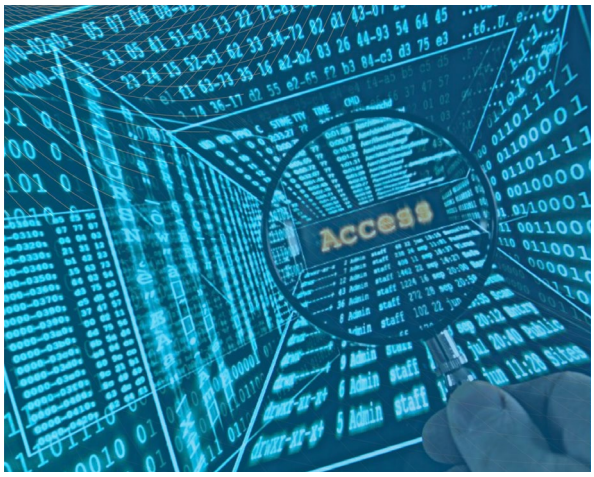
ULUSLARARASI SUİSTİMAL İNCELEME UZMANLARI DERNEĞİ
USIUD
2007

ACFE™
Association of Certified Fraud Examiners

Turkey Chapter - USIUD

Adli Bilişim ve Siber Suçlarla Mücadele Zirvesinin Ardından





14 MAYIS 2018
İSTANBUL

Kıvılcım Günbattı
ACFE Türkiye Eğitim Direktörü

14.05.2018 tarihinde Taksim Point Otel'de USİUD (Uluslararası Suistimal İnceleme Uzmanları Derneği) ACFE (Association of Certified Fraud Examiners) Türkiye tarafından gerçekleştirilen Adli Bilişim ve Siber Suçlarla Mücadele Zirvesi iki bölümden oluştu.

İlk bölümde Cyber Diligence Başkanı Yalkın Demirkaya "Siber Güvenlik, Siber Suçlar ve Adli Bilişim: Yeni Nesil Suistimal İnceleme Uzmanlarına ve Güvenlik Yöneticilerine Duyulan İhtiyaç" başlıklı sunumunda bilgi güvenliği ve endüstriyel casusluğa karşı koyma teknikleri, güncel risklere karşı adli bilişim metotları ve siber suçla mücadele araçları, soruşturma ve incelemede kullanılan güncel yöntemler hakkında bilgi ve deneyimlerini paylaştı.

İkinci bölümde suistimallerin tespit edilmesi ve delilendirilmesinde adli bilişim metotları ve teknolojinin etkin kullanımı konusunun tartışıldığı panel gerçekleştirildi. ACFE Türkiye Başkan Yardımcısı Cengiz Gümüştüs'ün moderatörlüğünü yaptığı panelde Yalkın Demirkaya'nın yanısıra bankacılık, sigortacılık, telekomünikasyon ve teknoloji sektörlerinden; **PwC Adli Bilişim Çözümleri Lideri Derya Etiz, KKB Veri Analizi ve Karar Destek Sistemleri Yöneticisi Dr. Emre Karaman, , SBM Sigorta Sahteciliklerini Engelleme Direktörü Salih Taşyon ve Dr. Mesut Demirbilek panelist olarak yer aldı.**

Açılış konuşmasını yapan ACFE Türkiye Başkanı Gökhan Yılmaz, suistimalin tespiti ve önlenmesinde adli bilişim araçlarının kullanımının önemine vurgu yaptı.

Başkan Yılmaz, Uluslararası Suistimal İnceleme Uzmanları Derneği'nin kurulduğu 2007 yılından bu yana suistimal inceleme faaliyetlerinin yürütülmesinde, bu alanda çalışacak uzmanların yetişmesinde, suistimal inceleme faaliyetleri ile ilgili etik ve hukuk düzeninin oluşturulması ve geliştirilmesi süreçlerinde ülke içinde öncü, lider ve referans kurum kimliğini sağlamak vizyonuyla hareket ederek, suistimale karşı mücadelede meslek mensuplarını ortak bir platformda birleştirme amacı doğrultusunda çalıştığını belirtti ve gerçekleştirilen etkinliğin önemine vurgu yapmak için aşağıdaki istatistikleri paylaştı.

ACFE tarafından yapılan araştırmalara göre, **adli bilişim metotlarını kullanan şirketlerde suistimallerin %52 oranında azaldığına ve vakaların %58 oranında daha hızlı tespit edildiğine** değinen Yılmaz, **suistimali gerçekleştiren kişilerin %84 oranında elekronik bir kaydı veya belgeyi tahrif ederek suistimalini sakladığını**, bunun da adli bilişim yöntemleriyle tespit edilebileceğini ifade etti.

Gökhan Yılmaz
ACFE Türkiye Başkanı

Yılmaz, ACFE Türkiye olarak 2015 yılında Türkiye özelinde gerçekleştirilen araştırma sonuçlarına göre, şirketlerin **%87 oranında veri analizi ve adli bilişim metotlarının suistimali tespit etmekte önemli olduğunu düşündüğünü**, ancak **sadece %21'nin bu yöntemleri kullandığını** ve **bu yöntemlerden yeterli verim alınamamasının nedenleri arasında en başta %43 ile uzman personel eksikliği olduğunu** vurguladı.

Yılmaz ayrıca, 2018 yılı Türkiye Suistimal Araştırması'nı başlattıklarını vurgulayarak, katılımcıları araştırmaya katkı sağlamaya davet etti (Araştırmaya suistimal.org adresinden katılabilirsiniz).

Yalkın Demirkaya'nın sunumunda öne çıkan hususlar ise şöyledi:

"Bilgi güvenliği ve suistimal risklerine karşı gelişmiş teknolojileri kullanmaya ihtiyacımız var"

Kurumların siber düşmanlarını tanıması, saldırı kapasitelerini ve kullandıkları teknikleri bilmesi çok önemli. Siber düşmanlar devlet istihbarat örgütleri olabileceği gibi özel kurumlar ve şahıslar da olabilir. Devletlerin istihbarat örgütleri özel şirketlere dönük fazla ilgi duymuyor, ancak diğer özel şirketlerin içinde bu yolla rekabet bilgisi toplamak isteyenler olabilir. Örneğin Ford firması yeni bir modelin geliştirilmesi sürecinde Ar-Ge'ye 2 milyar ABD Doları harcıyorken, bu bilgileri 10 milyon ABD Dolarına bir hackerdan satın almak, yasa ve etik dışı olmakla birlikte, başka bir firma için cazip olabilir ve endüstriyel casusluk yaygın bir durumdur.

"Şirketlerin en önemli ve acil işi, yönetimlerini bu alanda eğitmek"

Son zamanlarda en popüler saldırı tekniklerinin başında fishing (oltalama) yöntemi ve şirket e-postalarının ele geçirilmesi geliyor ve "siber savaş" da artan bir yoğunlukla devam ediyor ve bunun en yakın örneği Rusya ve Estonya arasında yaşandı. Endüstriyel casusluk vakalarında en çok adı geçen ülke olan Çin firmalarının malzemelerini sistemlerinde kullanan şirketlerin de ekstra dikkatli olmalarını tavsiye ediyorum.

Malware: Bunlar truva atları, keyloggerlar, arka kapılar gibi şirketlerin aktivitelerini takip eden zararlı yazılımlar ve bunların geçici bellekte yaşayan ve tespiti oldukça zor dosyasız türevleri var. Bu zararlı yazılımlar internetten bulaşabildiği gibi, şirket networküne kurulmak üzere ısmarlanan donanımın içinde de gelebiliyor.

Yalkın Demirkaya
Cyber Diligence Başkanı

Bilgisayarın anakartına veya klavyesine eklenmiş bir çip ve cep telefonu mekanizması sayesinde çalınan verilerin şirket ağına ihtiyaç duyulmaksızın ve dolayısıyla bir trafik oluşturmadığı için tespiti ve engellenmesi zor yöntemler bulunuyor. Şirket ağına eklenen basit bir ethernet kablosunda bile böyle bir sistemin bulunduğu vaka örneklerine rastlıyoruz.

Spyware: Anti-virus programlarının yakalayamayacağı bu yazılımların gayet etkili formları darknet üzerinden 100 ABD Dolarına satın alınabiliyor ve bunların bir de 10.000 ABD Dolarına satılan ve çok çok güçlü formları var.

Yalkın Demirkaya
Cyber Diligence Başkanı

Böcekle dinleme: Genellikle Ar-Ge programları, satın alma/birleşme gibi korunması gereken gizli bilgileri elde etmek için kullanılan bu yöntem, en basit haliyle şirketin temizliğini yapan bir çalışan kılığında yahut bir çalışanın işbirliğiyle şirkete girilip, bu böceklerin dinlenmek istenen alanlara yerleştirilmesine dayanıyor. Bu alanda teknoloji saldırganlara çok ileri imkanlar sağlıyor. Sadece dinleme yaparken aktif olan ve bunu da çok düşük bir enerji seviyesinde, çok düşük ısı ve sinyal yayarak yapabilen, sinyali yayılım şeklinde değil doğrusal bir çizgi halinde gönderen ve tam da bu doğrultudan yapılacak bir tarama olmadıkça tespit edilmesi neredeyse imkansız böcekler bulunuyor ve bunlar ancak ileri seviye ekipmanlar ve eğitimli uzmanlar tarafından tespit edilebiliyor.

Data hiding and encryption: Hedef alınan şirket verilerini şifreleyip saklayarak şantaj yapmaya dayanan bu yöntem son zamanlarda çok sık görülüyor.

"Adli bilişimde son zamanlarda kullanılan çeşitli teknolojik aletler ve yazılımların hiçbiri mükemmel değil, kullanım amacına göre avantaj ve dezavantajlara bakmak gerekir"

Her ihtiyaca cevap veren "hepsi bir arada" bir çözüm bulunmuyor. Çeşitli araçların çeşitli alanlarda birbirlerine üstünlükleri bulunabiliyor. Bir adli bilişim uzmanını marangoz ve sahip olduğu araçları da bir marangozun kullandığı araçlar olarak düşünebiliriz. Marangozlar kesme, delme, yontma gibi çeşitli işler için nasıl tek bir aletten değil, bu işler için özelleşmiş farklı aletler kullanıyorsa, adli bilişimde de farklı işler için özelleşmiş farklı araç ve teknikler bulunur.

Örneğin dosya filtreleme, zaman çizelgesi oluşturma ya da e-posta arama yapma gibi farklı görevler için özelleşmiş yazılımlar bulunur. Aynı işi yaptığı iddia edilen yazılımlar arasında da önemli ölçüde etkinlik ve güvenilirlik farkı olabilir. Ayrıca bilinçsiz bir seçimle, sırf çok sayıda fonksiyon barındırdığı için pahalı bir yazılım alınarak, ihtiyaç duyulmayan fonksiyonlar için para ödemek de anlamlı olmayabilir.

Dolayısıyla bilinçli bir seçim yapabilmek için, alınacak hizmet/yazılımlarından hangisinin ihtiyacı ne ölçüde karşıladığı ve maliyeti gibi çeşitli hususların göz önüne alınarak karar verilmesi gerekir.

Kurumların ellerindeki imkanlara ve güvenlik ihtiyaçlarının önceliklendirilmesine göre kurguladıkları, etkin kaynak yönetimine dayanan bir güvenlik stratejisine sahip olmaları bu bakımdan çok önemlidir.

"Dijital bir suistimal olayından ilk şüphelenildiğinde, vakayı bilmesi gerekenlerden (need to know) başka kimseyle paylaşmamak gerekir"

Çalışanlar olayı öğrendiklerinde panik olabilir, kendilerini koruma moduna geçebilir ve sorulduğunda tüm gerçekleri söylemeyebilirler. Hatta/suistimal yapan BT çalışanlarından biri olabilir. Bu nedenle konudan, yalnızca güvenilir bulunursa BT bölümündeki yöneticiye bahsedilmelidir.

Demirkaya, izlenmesi gereken vaka yönetim prosedürünü aşağıdaki şekilde tarif etti:

1. İlk Müdahale
    a. Dijital suç mahalinin incelenmesi
    b. Delil toplama yöntemlerinin uygulanması
    c. Dijital delillerin incelenmesi
2. Kontrol altına alma
    a. Saldırganın tanımlanması
    b. Saldırganın erişiminin duraklatılması
    c. Saldırganın erişiminin tamamen durdurulması
3. Hasarın onarılması
    a. Ne, nasıl, ne zaman ve kim tarafından yapıldı tespit etmek için detaylı inceleme
    b. Temizlik ve onarım

IT'nize soracağınız sorular neler olmalı:

- Delil toplamayı biliyor musun?
- Ram imajı almayı biliyor musun?
- Firewall'da belli bir bölgeyi bloke etmeyi biliyor musun?
- Fire wall loglarına bakıp giriş çıkış kotrolü yapabiliyor musun?
- En son o loglara ne zaman baktın ve en ilginç ne gördün?

"Fishing saldırıları çok popüler, o kişilere aitmiş gibi görünen adreslerden saldırıyorlar"

Bu yöntemde saldırganlar web sitenizden ya da Linkedin'den genel müdürünüzü, CFO'nuzu; üst düzey yöneticilerinizi bulduktan sonra, bu kişilere ait gibi görünen email adreslerini satın alarak bu adreslerden çalışanlara talimat gönderirler. Daha tehlikeli ve etkili olan başka bir yöntemde ise şirketteki bir veya birkaç kişinin hesabını ele geçirdikten sonra, o kişilerin email adresiyle kendilerinin fark etmeyeceği şekilde emailler göndererek tüm iş süreçleri ve bağlantılarını öğrenerek, yazışma içerikleri ve ekleriyle oynayarak paraların kendi hesaplarına gönderilmesini sağlarlar ve bazı durumlarda bu çok uzun bir süre fark edilmeksizin sürdürülebilir.

"Network güvenliği sağlamak için değişik teknikler, yazılımlar, donanımlar mevcut"

Anti-virüsler: Çalışma sistemlerinden dolayı tehditlerin ancak %20'sine cevap verebiliyorlar. En zayıf tarafları yeni ortaya çıkan tehditlere ayak uyduramamaları.

Firewall: Bugünlerde her network'ün önünde firewall var. Artık bu bir koruma değil. Artık saldırganlar firewall'ların etrafından dolaşıp geçiyor. Eğer satın aldığınız firewall'u kendinize uygun bir şekilde yapılandırabilirseniz, etkinliğini %80 oranında arttırabilirsiniz.

Yapılabilecek başlıca ayarlar ve alınabilecek önlemler: Güvenilmeyen e-posta sunucuları ya da iletişim bölgeleri ve iş ilişkisi içinde olunmayan ülkeler bloklanabilir, iç firewall'lar kullanılabilir, hassas bilgiler internete kapalı, sadece iç network'e bağlı bilgisayarlarda depolanabilir. İç tehditlere karşı sistem sıkılaştırma yapılabilir. İnternete çıkan bilgisayarlar, iç tehditlere karşı "silent runner" isimli yazılımla korunabilir.

"Saldırganların en tehlikelileri APT (advanced persistent threats)"

APT'ler hem maddi, hem teknik, hem insan kaynağı olarak güçlüler ve hedefe koydukları kişi ya da kurumun peşini bırakmıyorlar. Güçlüler, çünkü arkalarında genellikle devletler var. Bilgi çalma amacı için en çok bilgisayarları kullanıyorlar. Çok güçlü araçları da kullanıylar ve bazen hedef saptırmak için sıradan hacker'ların kullandıkları daha basit araçları da. Bunun dışında yerine göre dinleme böcekleri de kullanabiliyorlar. **Bu saldırganların bir noktada başarılı olacak bir saldırısını engellemek neredeyse imkansız, çünkü süreklilik arzeden, sonu gelmeyen bir saldırı tipi. O yüzden inceleme uzmanlarına düşen daha çok saldırıyı tespit edebilmek.** Bizler bu tür saldırıları tespit etmek için en etkili araç olarak 'network forensics' araçları kullanıyoruz. En etkili savunma sistemi ise 'intrusion prevention' sistemleri.

İzinsiz/zorla içeri girişleri tespit eden sistemler kullanılmalı. Bilgisayarlar ve workstation'lar sadece server'la konuşmalı, birbirleriyle konuşmamalı, konuşursa bunu saptamak ve araştırmak lazım. İzinsiz girişlerden korunmak mümkün, ama bunun için büyük bütçe, disiplin ve teknik bilgi lazım.

Böcek koyma, networke eklenen bir ethernet kablosu şeklinde kurulmuş harici cihazlarla dinleme gibi saldırıları, bunları tespit etme hizmeti veren firmalardan alarak engelleyebilirsiniz. Ancak bu hizmeti veren firmaların da çoğunda böcekleri belirleyebilecek yeterli araç gereç ve teknik bilgi yok. Bu alandaki teknoloji ve yöntemler çok hızlı gelişiyor ve bunu takip edebilmek için yüklü yatırımlar yapmak gerekiyor. Bu da verilen hizmetin fiyatının artması demek; ancak genelde hizmet alan firmalar yeterli düzeyde farkındalığa sahip olmadıklarından bu fiyatları ödemeye istekli değiller.

Soldan sağa: Yalkın Demirkaya, Derya Etiz, Dr.Emre Karaman, Salih Taşyon, Dr.Mesut Demirbilek, Cengiz Gümüştüs

Suistimallerin tespit edilmesi ve delillendirilmesinde adli bilişim metotları ve teknolojinin etkin kullanımı konusunun tartışıldığı panelde öne çıkan görüşler şöyleydi:

Dr. Mesut Demirbilek: Suistimaller bir anlamda kendi kurumlarımızın içerisindeki kanserli hücrelerdir. Çünkü kanserli hücreler zamanla gelişirler ve metastas yaparak kurumun/şirketin bütününü kapsamaya başlarlar ve onu ele geçirirler. Bu nedenle suistimalle yapılacak olan mücadele tam tanımıyla bir terörle mücadele gibi ya da bir suçla mücadele gibi önemlidir. Suistimal kapımıza gelene kadar suistimal ile ilgili bir şey yapmıyoruz. Suistimalin önlenmesinden tespitlerine kadar genellikle bize dokunmadıkça bir şey yapmıyoruz.

Telekom sektörü teknolojiyle yapılan suistimallerde ilk sırada gelen sektörlerden biridir. 15-20 sene öncesine gelene kadar en çok duyduğumuz telekom suistimallerinden biri kontör dolandırıcılığıydı. Daha sonra hayatımıza 3G/4G, internet, data girdi. Ürünler çoğaldı. İnsanların kullanımı kat kat arttı. Dışardan çok sayıda saldırı alıyorsunuz. Bu almış olduğunuz saldırılar, eğer başarılı olabilirlerse; sizin, şirketinizin veya müşterilerinizin paralarını bir şekilde alıyorlar, kullanıyorlar ya da sizi zarara sokuyorlar.

Şu an **Türkiye'de köylerde mezralarda bile özel kurulmuş data center gibi yerler var. İşleri güçleri suistimal olan, sabah saat 8 gibi mesaiye gider gibi giden ve akşam da 6'da çıkan, süreklilik arzeden şekilde maaşlı olarak oralarda çalışan insanlar var, bir sendika kurmadıkları kalmış.** Öyle ki; **neredeyse bu işle uğraşmayan gençlere de kız vermiyorlar** diyecek noktaya gelmişiz.

Dr. Mesut Demirbilek

Çok sayıda telekom fraud türü var. Ama en yaygın ve güncel olanı ve her şeyin başlangıcı diyebileceğimiz konu açık hatlar. Bir çok işlem, bankacılık faaliyetleri, sigortacılık faaliyetleri telefon ile yapıldığı için, terör faaliyetlerine varıncaya kadar pek çok suç bu açık hatlarla işleniyor.

Siber güvenlik konusunda özellikle önleyici ya da proaktif olmak oldukça önemli; çünkü reaktif tarafta kaldığınız zaman aslında birçok şeyi kaybetmiş oluyorsunuz ve artık geriye bu kayıplarınızı geri almaya çalışmaktan başka bir şey kalmıyor. Aslında işin %80-90'lık bölümü kesinlikle proaktif olmakta saklı.

Sektörler arası ilişki son derece önemli. Telekom açısından bakacak olursanız. Biz finans kuruluşlarıyla çok yoğun çalışıyoruz. Suistimalle etkin mücadele farklı sektörlerin ortak çalışmasını gerektiriyor. Bunun diğer önemli bir paydaşı ise tabi ki kamu. Kamuda da ağırlıklı olarak emniyet, jandarma, kolluk kuvvetleri ya da istihbarat birimleri ile görüşülebiliyor. Neticede ortak amaç, kötülere karşı birlikte mücadele vermek.

Salih Taşyon: Sigorta poliçesi bilgisi demek her türlü bilgi ve bilgi demek de para demek. Bir suistimalci poliçe bilgilerine ulaştığı anda en basit yolla poliçe sahibini arayarak ve sahip olduğu bilgileri kullanarak sosyal mühendislikle poliçenizi yenileyelim diyerek poliçe sahibinin kredi kartı bilgilerine ulaşabilir.

Sigorta veritabanında da 15 yıllık bir data var. Bugün bu dataya bakarak biz biliyoruz ki; yarın Taksim Point Otel önünde biri beyaz biri sarı renkli iki araba çarpışacak, beyaz renkli araba içindeki kişi 35 yaşlarında olacak…Bunu biliyoruz, neden? Haftada 65bin kaza oluyor Türkiye'de. Biz bunu temelde kişileri, tamirhaneleri skorlamak ve skorlarla da kişilere, şirketlere özellikle kendi datalarıyla elde edemeyecekleri şekilde uyarılarda bulunmak amacıyla kullanıyoruz. **Sigorta dünyasında, bir siber saldırganın poliçe bilgilerini ele geçirmesinin, her türlü suistimali gerçekleştirmek üzere ihtiyaç duyacağı tüm bilgi ve imkana sahip olması demek** olduğunu dikkate aldığımızda, poliçe bilgileri başta olmak üzere müşteri bilgilerinin güvenliğinin sağlanmasının ne kadar kritik bir konu olduğu anlaşılacaktır.

Dr. Emre Karaman: Sahteciliği önlemek için kural bazlı ya da yazılım bazlı çok çeşitli çözümler var. İçinde yaşadığımız dijitalleşme çağında yapay zekanın kendine suistimalle mücadele alanında da yer bulduğunu görüyoruz. **Yapay zeka bu alanda insanların yerini belki hiçbir zaman %100 olarak alamayacak olsa da, sağladığı otomasyon ve ileri seviyede veri analizleriyle insan zekasını destekleyen çok önemli bir araç olarak yerini aldı.**

Salih Taşyon
SBM Sigorta Sahteciliklerini Engelleme Direktörü

Büyük bankalar bazı problemlerle hiç karşılaşmazken, daha küçük ölçekli ve dolayısıyla daha riskli segmentlere hitap eden bankaların durumları farklı olabiliyor. Kurumlar arasındaki bilgi paylaşımı çok önemli, çünkü **dolandırıcılar kendi aralarında muazzam bilgi paylaşımı yapıyorlar.** Yasadışı forumlar ve dark web üzerinden "bu kurum böyle bir tedbir almış, bu tedbir nasıl geçilir" gibi konuları birbirleriyle paylaşıyorlar, **dolayısıyla** iyi adamların, yani kurumlarımızın da bunlara karşı iş birliği yapması çok önemli.

Dr. Emre Karaman
KKB, Veri Analizi ve Karar Destek Sistemleri Yöneticisi

Sistemlerimiz var, firewall var bizi korur zannediyoruz. Ama bunları doğru bir şekilde kullanmıyorsanız, kontrollerin sürekliliğini, geçerliliğini takip etmiyorsanız daha kötü. Hiç kontrolünüz olmasa belki en azından "hiç kontrolüm yok uyanık kalayım" diyeceksiniz.

KKB olarak biz bankacılık alanında ulusal sistem kuruyoruz, ama sektörler arası iş birliği de çok önemli. Çünkü **suistimalle mücadele bir rekabet değil, işbirliği alanı.**

Derya Etiz: Telekom ve sigorta şirketlerinin suistimale karşı teknoloji kullanımında oldukça ileri bir noktada olduğunu görüyoruz, ama diğer şirketlerin daha kat edecek çok yolu var. **PwC 2018 suistimal araştırmasında suistimallerin %52'sinin içeriden, yani çalışanlar tarafından yapıldığını; dışarıdan yapılanların ise %60'tan fazlasının bizim "frenemies" olarak tanımladığımız müşteri, tedarikçi gibi bir üçüncü parti tarafından gerçekleştiğini görüyoruz.** Dolayısıyla, suistimallerin tespiti noktasında karşımızda çoğunlukla verisi elimizde olan ve bu bakımdan tespit edilmesi daha kolay bir suistimalci profili var ve bu imkanı kullanmak gerekiyor. Bilgi güvenliği açısından finansal hizmetler, telekom ve sigortacılık sektörlerinin büyük ölçüde regüle olduğunu ve bundan dolayı belli bir bilgi güvenliği olgunluk seviyesinde olduğunu görüyoruz. Bunların olmadığı sektörlerde ise ISO sertifikaları ile bir bilgi güvenliği olgunluk seviyesi, bir yönetim programı oluşturulmaya çalışıldığını görüyoruz.

Derya Etiz
PwC, Adli Bilişim Çözümleri Lideri

Katılımcılarımızın ACFE Türkiye Yönetim Kurulu üyeleriyle hatıra fotoğrafı

Teşekkür

Adli Bilişim ve Siber Güvenlik Zirvesi, ACFE Türkiye Eğitim ve Organizasyon Komitesi tarafından, değerli konuşmacılarımızın gönüllü iştirakleri, zirve ana sponsorumuz PwC Türkiye, etkinlik sponsorlarımız Esfor Güvenlik Danışmanlığı, EMT Electronics ve seminer sponsorumuz Cyber Diligence'ın katkıları ve değerli konuklarımızın zirvemize gösterdikleri teveccüh sayesinde gerçekleştirilmiştir.

Bu vesileyle ACFE Türkiye Yönetim Kurulu olarak:

Ana konuşmacımız Yalkın Demirkaya'ya, panelistlerimiz Derya Etiz, Dr. Emre Karaman, Dr. Mesut Demirbilek, Salih Taşyon ve panel moderatörümüz Cengiz Gümüştüs'e ve tüm sponsorlarımıza çok teşekkür ediyoruz.

Yanısıra, tüm değerli konuklarımıza zirvemize gösterdikleri teveccüh ve zirve boyunca eksilmeyen ilgi ve dikkatleri için müteşekkiriz.

Bu e-kitapçık ACFE Türkiye Eğitim & Organizasyon Komitesi ve Yayın & Standartlar Komitesi işbirliğiyle hazırlanmış olup, zirvenin organizasyonu ve e-kitapçığın hazırlanmasındaki gönüllü katkıları nedeniyle Eğitim Direktörümüz Kıvılcım Günbattı'ya ve e-kitapçığın hazırlanmasındaki gönüllü katkıları nedeniyle Yayın ve Standartlardan sorumlu YK Üyemiz Av.Dr. Bülent Balkan ve Komite Başkanımız Çiğdem Gürer'e ve emeği geçen herkese teşekkür ediyoruz.

USİUD - ACFE Türkiye Hakkında

USİUD (Uluslararası Suistimal İnceleme Uzmanları Derneği) yaklaşık 150 ülkeden 85.000 üyesi ile dünyanın en büyük suistimal ile mücadele örgütü olan **ACFE'nin (Association Certified Fraud Examiners)** Türkiye temsilcisi olarak kurulmuştur ve kuruluşundan bu yana suistimal inceleme faaliyetlerinin yürütülmesinde, bu alanda çalışacak uzmanların yetişmesinde, suistimal inceleme faaliyetleri ile ilgili etik ve hukuk düzeninin oluşturulması ve geliştirilmesi süreçlerinde ülke içinde öncü, lider ve referans kurum kimliğini sağlamak vizyonuyla hareket eden mesleki bir örgüttür.

USİUD bu misyonunu yerine getirirken başta mesleği icra edenlere, bu mesleği seçeceklere, suistimale maruz kalan özel sektör ve kamu kuruluşlarına, ülkeye ve topluma doğrudan veya dolaylı katkıda bulunmaktadır.

Derneğimiz hakkında daha fazla bilgi edinmek ve üye olmak, güncel faaliyetlerimiz ve etkinliklerimizden haberdar olmak için **usiud.org** adresini ziyaret edebilir, sosyal medya hesaplarımızı takip edebilirsiniz.

Bayar Cad. Şehit Mehmet Fatih Öngül Sok. Bağdatlıoğlu Plaza
No:3 K:8 | Kozyatağı | İstanbul | Türkiye
Telefon : +90 850 532 90 64 | Faks: +90 216 706 01 26 | www.usiud.org | bilgi@usiud.org