IDEA STUDIES Journal
International Journal of Disciplines Economics & Administrative Sciences Studies
Open Access Refereed E-Journal & Indexed & Puplishing
e-ISSN:2587-2168

Volume: 6 / Issue: 20 / Page: 498-508
Doi No: http://dx.doi.org/10.26728/ideas.301
Arrived : 20.06.2020
Published: 30.08.2020
RESEARCH ARTICLE

KİŞİSEL VE KURUMSAL VERİ VE BİLGİ GÜVENLİĞİ AÇISINDAN SOSYAL MÜHENDİSLİĞİN ÖNEMİ

The Importance Of Social Engineering In Personal And Institutional Data And Information Security

Öğr. Gör. Cevdet ÖZMEN [1]

Reference: Özmen, C. (2020). "Kişisel ve Kurumsal Veri ve Bilgi Güvenliği Açısından Sosyal Mühendisliğin Önemi", *International Journal of Disciplines Economics & Administrative Scienves Studies*, Vol:6, Issue:20; pp:498-508

ÖZET

Kişisel verilerin korunması yalnızca 07.04.2016 tarih ve 29677 Sayılı Resmî Gazetede 6698 numara ile yayımlanan Kişisel Verilerin Korunması Kanunu kapsamı çerçevesinde değerlendirilemeyecek kadar karmaşık ve birçok farklı disiplin (sosyoloji, psikoloji, sosyal-psikoloji, kriminoloji, toplum bilimi vb.) ile birlikte ele alınması gereken bir kavramdır. Yine, kurumsal verilerin korunmasında da kişisel verilerin korunmasına benzer durum ve hassasiyetler söz konusudur. Sosyal Mühendislik ise bu alanların başında yer almaktadır. Olguları ve süreçleri değerlendirirken karşılıklı etkileşimin önemi kişisel ve kurumsal veriler ile Sosyal Mühendislik arasında da kendini göstermektedir. Bu çalışmanın amacı, gün geçtikçe daha çok sayısallaşan dünyamızda, hiç olmadığı kadar önem arz eden veri ve veri güvenliği bağlamında kişisel ve kurumsal verilerin korunması hususları ele alınırken Sosyal Mühendislik'den bağımsız olarak irdelenemeyeceğinin daha net anlaşılabilmesine katkı sunmaktır. Literatür araştırması yapılarak gerçekleştirilen bu çalışmada, kişisel ve kurumsal verilerin korunmasında hukuksal düzenlemeler ve teknolojik önlemlerin yanı sıra, eğitilmiş insan kaynağının halen en önemli ve hassas unsurların başında yer aldığı görülmüştür. Bu çalışmada, kişisel ve kurumsal verilerin korunmasına yönelik düzenleme ve çalışmalar yapılırken kesinlikle Sosyal Mühendislik'in göz ardı edilmemesi gerektiği sonucuna ulaşılmıştır.
Anahtar Kelimeler: kişisel verilerin korunması, kurumsal verilerin korunması, sosyal mühendislik, veri güvenliği, bilgi güvenliği

ABSTRACT

The protection of personal data is a concept that is too complex to be evaluated only within the framework of the Law on Protection of Personal Data published in the Official Gazette with a number 6699 on April 07, 2016 and must bu dealt with in many different disciplines (e.g. sociology, psychology, social-psychology, criminology, social science) and fields. Similarly, there are similar situations and sensitivities in the protection of institutional data as protection of personal data has. Social Engineering is at the top of these fields. The importance of interactions in evaluating cases and processes is also evident between personal and institutional data and Social Engineering. The aim of this study is to contribute more clearly to the fact that the protection of personal and institutional data in the context of data and data security, which is more important than ever in our digitalizing world, cannot be examined independently from Social Engineering. In this study, which was carried out by reviewing the literature, it was observed that trained human resources are still among the most important and sensitive elements in addition to legal regulations and technological measures in the protection of personal and corporate data. In this research, it is concluded that Social Engineering should definitely not be ignored during the the regulations and studies for the protection of personal and institutional data.
Key words: personal data protection, institutional data protection, social engineering, data security, information security

1. GİRİŞ

Gün geçtikçe daha çok sayısallaşan dünyamızda, hiç olmadığı kadar önem arz eden veri ve veri güvenliği bağlamında kişisel ve kurumsal verilerin korunması konusu ele alınırken birçok parametrenin göz önünde tutulması gerekmektedir. Endüstri 4.0'ın temel bileşenleri arasında yer alan ve en önemlilerinden olan Nesnelerin İnterneti (Internet of Things- IoT) yapısında var olan ve akıllı (smart) cihazların birbirleriyle iletişim kurmaları, sürekli ve anlık olarak bilgi aktarması süreçlerinde olduğu gibi artık hiçbir şey bir birinden bağımsız ve habersiz olmayacaktır. İşletmeler için de benzer yaklaşımlar söz konusudur: İşletmelerin dış çevreden bağımsız olarak hareket etmeleri rekabet etme gücünü ortadan kaldırıp, sürdürülebilir karlılık ve verimliliği negatif yönde etkilemektedir. Entropi ile de ancak "açık sistemler" sayesinde baş etmek mümkündür.

Orta vadede Endüstri 4.0'ın kişiler ve işletmeler üzerindeki etkilerinin daha belirgin bir hâl alabileceğini söylemek mümkündür. Endüstri 4.0'ın sağlıklı işleyebilmesi açısından ana omurgayı ise veri ve bilgi güvenliğinin oluşturacağını söylemek mümkündür. Oysa yapılan çeşitli araştırmalar bize gösteriyor ki, henüz veri ve bilgi güvenliği problemleri arzu edilen düzeyde çözülebilmiş değildir. Sayısallaşma, bilgisayar ve internet platformları var olduğu sürece bu güvenlik sorunları hep

1. Giresun Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı Doktora Öğrencisi, Giresun/Türkiye ORCID: 0000-0002-8820-6032

var olacak gibi duruyor. Bu durumdan hareketle güvenliğin tam manasıyla sağlanmasının şimdilik söz konusu olmadığı çıkarsanabilir. Güvenlik önlemlerine yönelik güncel çalışmalarda zararın giderilmesinden ziyade, zarara hiç uğranmaması hedeflenmekte ve bu doğrultuda reaktif önlemlerin yerini proaktif önlemler almaktadır.

Bu çalışmada, kişiler ve kurumlar açısından veri ve bilgi güvenliğinin önemi üzerinde durulmuştur. Veri ve bilgi güvenliğinin yalnızca teknolojik yatırımlar ve önlemler ile alınmasının söz konusu olamayacağını, insan unsurunun halen çok etkin ve önemli ama diğer taraftan da en zayıf halkayı oluşturduğunu, insan unsuru söz konusu olduğu vakit güvenliğin sağlanabilmesi için ise Sosyal Mühendisliğin (SM) ne olduğunun bilinmesi ve onun negatif yönlerine karşı ne tür önlemlerin alınabileceği tartışılmıştır.

SM çatısı altında basit ama etkili önlemler ile hem SM atakları hem veri ve bilgi güvenliği alanlarına yönelik birçok güvenlik açığının giderilebileceği düşünülmektedir. SM bileşenleri ve SM saldırı teknikleri açıklanarak, teknoloji okur-yazarlığının arttırılması ve alınabilecek önlemlerin belirlenmesi açısından bu çalışmanın yararlı olacağı düşünülmektedir.

2. KAVRAMSAL ÇERÇEVE

2.1. Veri

Veri ham'dır. Sadece var olur ve varlığının ötesinde bir önemi yoktur. Herhangi bir formda bulunabilir, kullanılabilir ya da kullanılamaz. Kendi başına bir anlamı bulunmaz (Ahsan ve Shah, 2006). Veri genel olarak yorumlanmaya ve insanların anlayabilecekleri hale dönüştürülmeye muhtaç ham gerçekler olarak tarif edilmektedir. Ok (2013: 20) veriyi, işlenmemiş bilgilere verilen ad olarak tanımlamakta, sayı, sembol, harf gibi ifadelerden oluşabildiğini ve yine tek başına bir anlam ifade etmediğini belirtmektedir. Yalçınkaya (2013) ise veriyi, "bir gerçek hakkında değerler sunan herhangi bir karakter dizisi" olarak tanımlamakta ve veri'nin bize ne yapmamız gerektiğini söylemediğini ancak enformasyon yaratmak için vazgeçilemez bir kaynak hammadde olmasının onu oldukça önemli kıldığını belirtmektedir (s. 38). Şu halde veri, üzerinde çalışılarak çeşitli sınıflamalar, gruplamalar yapılan, bir nevi işlemden geçirilerek enformasyon oluşturmaya temel teşkil eden ve sonrasında bilgiye dönüşecek olan sürecin ana yapı taşlarını oluşturmaktadır.

2.2. Enformasyon

Enformasyon, ilişkisel bağlantı yoluyla anlam verilmiş verilerdir. Bu "anlam" faydalı olabilir, ancak olmak zorunda değildir (Ahsan ve Shah, 2006). Enformasyon, bir karar verme sürecinde, erişilecek sonuçları kestirmek ya da eldeki veriler ışığında bir işlem yapmak amacıyla gereklidir. Buradan hareketle enformasyonu, organize edilmiş bir veri seti olarak tanımlamak mümkündür (Ok, 2013: 20). Verinin derlenip düzenlenerek belirli bir amaca yönelik olarak organize edilmesi enformasyonu oluşturur (Yalçınkaya, 2013: 38). Enformasyon, verinin işlenmiş ancak henüz (tam olarak) bilgiye dönüşmemiş halidir. Enformasyon aynı zamanda eldeki verilerin kısmen de olsa düzenlenerek çeşitli yargılara ulaşabilmek için bir çeşit ön bilgi edinimi/aktarımı olarak da ifade edilebilir. Diğer yandan, bu süreci "kısmi bilgilendirme" olarak tanımlamak da mümkündür.

2.3. Bilgi

Bilgi anlamlandırılmış enformasyon olarak tanımlanmaktadır (Ok, 2013: 19). Veri, doğrudan gözlenebilir veya açıklanabilir içerikleri tarif ederken, enformasyon, analiz edilmiş verileri temsil eden içeriktir (Dalkır, 2011 Akt: Yazıcıoğlu, Borat ve Kılıç, 2014: 13). Bilgi ise, uygun enformasyon topluluğudur, öyle ki amacı faydalı olmaktır. Bilgi deterministik bir süreçtir. Birisi bilgileri "ezberlediğinde", o zaman orada bilgi birikimi oluşur (Ahsan ve Shah, 2006). Platon'a göre ise bilgi, gerekçelendirilmiş doğru inançtır (Musgrave, 1993 Akt: Uğraş, 2015: 18).

2.4. Veri ve Bilgi Güvenliği

ISO (2016) tanımına göre bilgi güvenliği; bilginin gizlilik, bütünlük ve kullanılabilirliğinin korunmasıdır. Ayrıca, orijinallik, hesap verebilirlik, reddedilmeme ve güvenilirlik gibi diğer

özellikler de söz konusudur. Veri ve bilgi güvenliği söz konusu olduğunda temel olarak kişisel (personal/individual) veri/bilgi güvenliği akla gelmekle birlikte esas olan kurumsal (institutional) veri/bilgi güvenliğinin sağlanmasıdır.

Bilgi güvenliği (information security), bilgilerin güvenliğinin sistemli bir şekilde korunmasıdır. Kurum faaliyetlerinin sürekliliğini sağlamak üzere bilgilerin olası her türlü tehlike ve tehditlere karşı korunmasıdır (Çubukçu, 2018: 3). Bunu başarabilmek için başta bilgisayar sistemleri ve insan kaynakları yönetimine odaklanmak gerekmektedir.

Bilgi güvenliğinin temel amacı, elektronik veya diğer ortamlarda var olan her nevi bilginin gizliliğini (confidentiality), bütünlüğünü (integrity) ve kullanılabilirliğini (availability) süreklilik arz edecek şekilde sağlamaktır (Bestel, 2008 Akt: Baktır, 2013: 116).

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişimi, kullanımı, değiştirilmesi, ifşa edilmesi, ortadan kaldırılması, el değiştirmesi ya da hasar verilmesini önlemek olarak tanımlanabilir ve "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel bileşenden meydana gelir (Puhakainen, 2006 Akt: Keser ve Güldüren). Pesen (2015)'e göre bu bileşenleri şu şekilde açıklamak mümkündür:

Gizlilik: Bilginin yetkisiz kişilerin eline geçmeme ve yetkisiz erişime karşı korunmasıdır.

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştiril(e)memesidir.

Erişilebilirlik: Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir olmasıdır.

Bu üç temel güvenlik bileşeninden (bu bileşenlere sonraki çalışmalarda *doğrulama, yetkilendirme* ve *inkâr edememe* kıstasları da ilave edilmiştir) herhangi biri zarar görürse sonuç olarak güvenlik zaafiyeti ortaya çıkmış olacaktır. *Sistem Yaklaşımı*'nda parçalar bütünü temsil etmektedir. Her parça kendi içerisinde önemlidir lâkin tüm parçaların birlikte ele alınması daha önemli bir durumu ifade etmektedir. Bilgi güvenliğini vücudun hayati organları gibi düşünecek olursak; her hayati organ birbiriyle iletişim halinde ve biri diğerini destekleyici durumdadır. Herhangi birinin yetersiz çalışması ya da görevini yerine getirmemesi yaşamın sonlanması olasılığını/riskini doğuracaktır.

Bilgi güvenliğinin bir "varlık" türü olarak ele alınması dikkat çekicidir. İşletmeler için artık veri ve bilgi, özenle korunması gereken bir değerdir. Birçok işletme açısından bu durum maddi varlıklara denk tutulmaktadır. Veri ve bilgi güvenliğini sağlayamayan işletmeler için müşteri memnuniyetsizliği söz konusu olabilmektedir. Bu durum en basit yanıyla; işletme güvenirliğinin azalması, rekabet gücünün yok olması, istatistiksel verilerin hazırlanamaması, tüketici alışkanlıklarının ortaya çıkartılamaması gibi birçok zafiyetin oluşmasına sebebiyet verebilmektedir. Bu ve benzeri nedenler ile işletmeler açısından veri ve bilgi (güvenliği) her geçen gün daha da kıymetli varlıklar haline dönüşmektedir. Öyle şirketler var ki, veri varlıklarına biçilen değerler, maddi varlıklarının yüzlerce katı olabilmektedir. Özellikle sosyal medya mecrasından bildiğimiz Facebook, Whatsapp, Instagram, Google bu şirketlere örnek olarak gösterilebilir. Bu şirketlerin *uygulamaları* sayesinde veri ve bilginin esas güç olduğunun farkına çok daha kolay varabilmekteyiz.

Bilgi değerleri, entelektüel sermaye ve soyut varlıklar açısından genellikle ekonomi literatüründe şu şekilde kullanılmaktadır; *bilgi varlıkları* (knowledge assets), yönetimde *entelektüel sermaye* (intellectual capital) ve muhasebede *maddi olmayan varlıklar* (intangible assets) (Yazıcıoğlu vd., 2014: 5).

Bilgi güvenliği çok çeşitli alanları ilgilendirmekle birlikte, genel olarak; veri güvenliği, ağ güvenliği, kullanıcı güvenliği, kimlik ve erişim güvenliği, uygulama (application) güvenliği, sanallaştırma ve bulut bilişim ve daha geniş anlamda ise güvenlik yönetimi gibi başlıkları kapsamaktadır.

Bilgi güvenliği alanında standart geliştirme işlemleri ilk olarak 1993 yılında İngiliz Standartlar Enstitüsü BS-779 standardı ile başlamış, güncellemeleri ise 2002 yılına kadar devam etmiştir. 2000 yılında ise BS7799-1, ISO (International Organization for Standardization) tarafından yapılan güncellemeler ile ISO/IEC-17799 adını almış ve sonrasında ise ISO/IEC:27001 adı ile son halini

almıştır (Sağıroğlu ve Alkan, 2007 Akt: Yiğitbaşı, 2015: 65). ISO'nun bu yönde değişik sektörlere yönelik çalışmaları ve güncellemeleri ağırlıklı olarak 27000 serisi üzerinden devam etmektedir.

Bir kurumdaki güvenlik seviyesini o kurumda bulunan en en zayıf halka belirlemektedir (Kara, 2018: 160). Güvenlik zincirindeki bu en zayıf halka genellikle insan unsurudur. Bazı araştırmalara göre, bilgi güvenliğine yönelik olarak düzenlenen güncel saldırıların yarısına yakın kısmı yukarıdaki nedenlerden ötürü insan faktörü üzerinden sosyal mühendislik girişimleri olarak gerçekleştirilmektedir.

2.5. Sosyal Mühendislik

Sosyal mühendislik, bilgi toplamak amacıyla güvenlik sistemlerini atlamak için insan zayıflığından yararlanma teknikleri olarak tanımlanmaktadır (Mitnick ve Simon, 2002 Akt: Mouton, Malan, Kimppa ve Venter, 2015: 115). Daha çok, insanın psikolojik yönünü ele alır ve insani zayıflıklardan faydalanır.

İnsanları "hack"leme olarak da bilinen sosyal mühendislik, çalışanları ve tüketicileri kimlik bilgilerini açıklamada kandırma ve daha sonra bu bilgileri ağlara veya hesaplara erişmek için kullanma sanatıdır (Conteh, 2016: 435). Sosyal mühendislik, insan faktörünü kullanan saldırı tekniklerinden veya kişiyi etkileme ve ikna etme yöntemlerinden faydalanarak, normal şartlarda bireylerin gizlemeleri, paylaşmamaları gereken bilgi ve belgeleri bir şekilde ele geçirme sanatıdır (Tübitak Bilgem, 2018 Akt: Kara, 2018: 160).

3. ARAŞTIRMANIN METODOLOJİSİ

3.1. Araştırmanın Amacı ve Önemi

Yapılan literatür araştırmasında veri/bilgi güvenliği ile sosyal mühendisliği ilişkilendiren yeterli çalışmanın olmadığı tespit edilmiştir. Veri ve bilgi güvenliğine yönelik önlemlerin genellikle teknolojik önlemler ile sağlanabileceği kanati yaygındır. Oysa daha kolay, daha az maliyetli ve hızlı olması bakımından veri ve bilgi güvenliğine yönelik yapılan saldırıların son zamanlarda sosyal mühendislik aracılığıyla yapıldığı çeşitli araştırmalarla ortaya konulmuştur. Bu çalışmanın temel amacı; kişisel ve kurumsal verilerin korunmasının yanı sıra bilgi güvenliğinin sağlanmasına yönelik çalışmalarda sosyal mühendisliğin önemine dikkatleri çekmektir. Alınabilecek basit ama etkili önlemler ile kişi ve kurumların kendilerini önemli ölçüde bu tür saldırılara karşı koruyabilecekleri öngörülmektedir.

3.2. Araştırma Yöntemi

Yaklaşık altı ay kadar süren kaynak taraması sonucu özellikle sosyal mühendisliğe yönelik olarak hazırlanmış yazı ve yazarların ortak görüşlerine yer verilerek oluşturulan bu çalışmada, karşılaştırmalı tablolar oluşturularak sosyal mühendislikle ilgili (yüksek oranda fikir birliği ile kabul edilen) vektör ve bileşenlerin açıklanması betimsel ve analitik bir yaklaşımla açıklanmaya çalışılmıştır. Betimsel yaklaşım daha çok mevcut (şimdiki) durumu açıklamaya çalışırken, analitik yaklaşım ise daha ziyade ulaşılmak istenilen (hedef) noktayı açıklamaya çalışır. Kpssnotlar.com web sitesinde ise analitik yaklaşım; gelecekte ortaya çıkması olası durumlardan hareket edilerek ihtiyaçların belirlenmesi, eleştirel düşünceden hareketle çözüm aranması şeklinde açıklanmaktadır. Açıklamada ayrıca, örnek olarak, teknolojik gelişmelerin neleri değiştireceği ve toplumda nelerin gelişeceği üzerinde durulduğu da ifade edilmektedir.

4. SOSYAL MÜHENDİSLİK

Sosyal mühendislik aslında tüm zamanların başından beri kullanılmaktadır. Yaratılan ilk insan olan Adem ve Havva'nın "İlk Günah"a düşmesi, yılanın ikna gücü olmadan mümkün olamazdı. III. Amenhotep'in askeri güç kullanmadan, Mısır'ın Suriye ve Filistin üzerinde hâkimiyeti diplomatik beceriyle başarıldı. Yunanlılar bile Truva şehrini fethetmek için sosyal becerilerini kullanarak, Ulysses komutasında Truva Atı'nı inşa etmiş ve bu şekilde şehre girebilmişlerdi. Yine benzer bir

şekilde, ikna ve "aldatma"nın önemi, San Tzu tarafından "Savaş Sanatı"nda açıklanmaktadır (Şerban ve Şerban, 2014: 6).

Sosyal Mühendislik, hassas bilgi edinmek, yetkisiz altyapıya ve tesislere erişmek için kullanılan bir aldatma şeklidir. Tüm sosyal mühendislik girişimlerinin teknoloji temelli aldatma veya insan temelli aldatma olarak sınıflandırılabileceği iki ana kategori bulunmaktadır (Thapar, Akt: Conteh, 2016: 436). Sosyal mühendislik saldırılarında her iki kategorinin ayrı ayrı kullanılabilmesinin yanı sıra bazı durumlarda her iki kategori birlikte de (eş zamanlı ya da sıralı) kullanılabilmektedir.

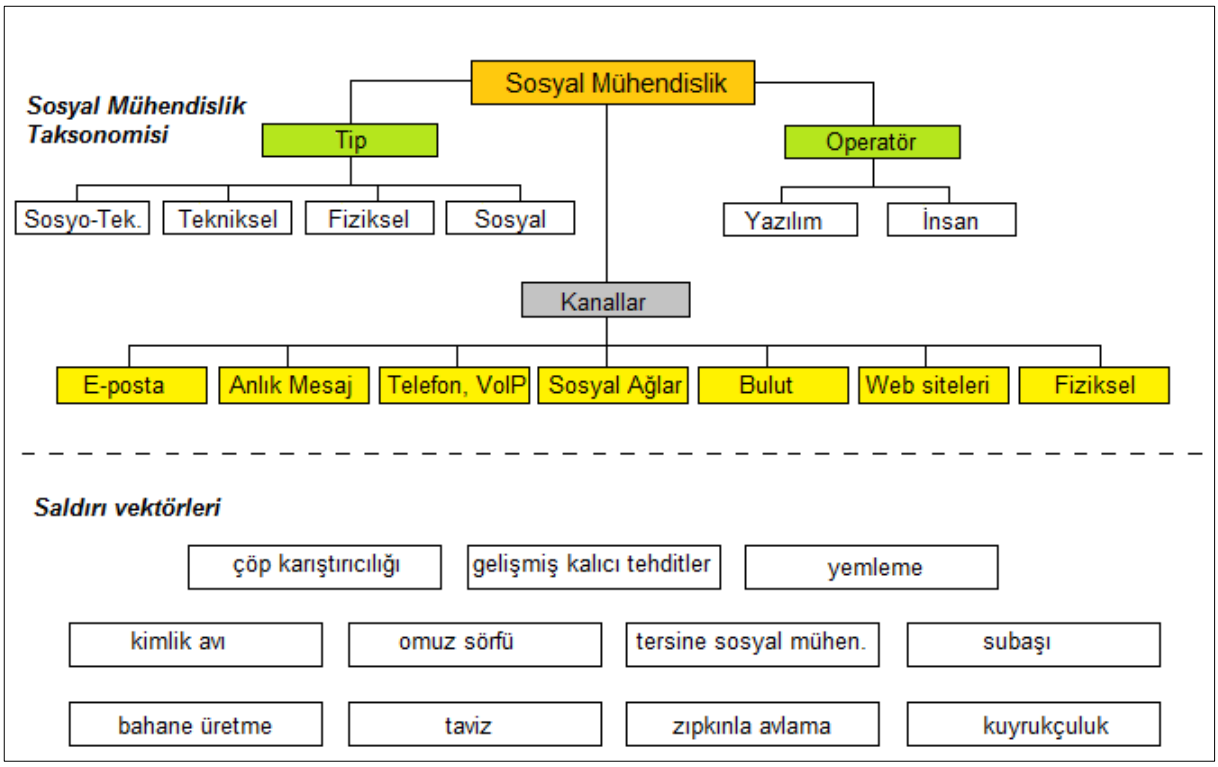
Sosyal mühendislik yöntemleri çok çeşitlidir ve bunları kullanan insanlar bu işi son derece ustaca yaparlar. Bu teknik, herkesin yapamayacağı, istisnai iletişim becerilerini kullanarak, hassas bilgiyi manipüle etmek/elde etmek ya da insanların kişisel özelliklerini keşfederek onları ikna etmek için kullanılmaktadır. Bu doğrultuda, insana özgü, insanın doğasından kaynaklı özelliklerden de faydalanılır (Şerban ve Şerban, 2014). Bu özellikler; ihtiyacı olana yardım etme, karşılık verme, benzer muamelede bulunma, iyiliğe iyilikle cevap verme, nezakete nezaketle karşılık verme, önemli biriymiş gibi davranma ihtiyacı, iltifat veya övülmeye bir tür (iyilikle) karşılık verme, kızgın olduğu bir kişi ya da kurumdan hınç alma girişimleri vb. kapsamaktadır.

4.1. Sosyal Mühendislik Saldırıları

Bir sosyal mühendislik saldırısı, siber ataklardan farklı olarak, bir kişi ya da işletmenin bilgi ve bilgi sistemlerini tehlikeye atmak, manipüle etmek veya değiştirmek için sosyal becerilerin kullanılmasını içerir. Sosyal mühendislik saldırıları siber ve teknolojik saldırılardan bağımsız değildir fakat teknolojik engelleri teknik bilgi ve donanımla aşmak yerine, daha kolay ve az maliyetli olan insan faktöründen faydalanarak amacına ulaşmaya çalışır. Özellikle küçük ve orta ölçekli, kurumlaşamamış işletmelerin bu tür saldırılara maruz kalma riski daha yüksektir. Bu tür ataklar, büyük ve gelişmiş şirketlere yönelik olarak da düzenlenmekle beraber, kolay hedef olan KOBİ'ler saldırganların daha çok tercih ettikleri işletmelerdir. KOBİ'lerin bu alanda yeterli insan kaynağının olmayışı, teknolojik önlemlerin alınmasına yönelik yeterli bütçe ayıramamaları, güncel tehditleri algılamada geç kalmaları bu tür saldırılara maruz kalmalarının ana sebeplerini oluşturmaktadır.

Krombholz, Hobel, Huber ve Weippl (2014)'e göre bilgisayar destekli sosyal mühendislik sanatında saldırılar tip olarak dört farklı kategoriye ayrılmaktadır: Fiziksel, teknik, sosyal ve sosyo-teknik yaklaşımlar. Operatör (araç) olarak ise; yazılım (software) ve insan faktörü şeklinde ikiye ayrılmaktadır. Saldırı kanalı olarak en çok kullanılanlar ise; e-posta, anlık mesajlaşma, telefon ve "ip" üzerinden sesli görüşme, sosyal ağlar, "bulut", web siteleri ve fiziksel erişimden oluşmaktadır. Yine en çok tercih edilen saldırı vektörleri ise; çöp karıştırıcılığı (dumpster diving), gelişmiş kalıcı tehditler (advanced persistent threat), yemleme (baiting), kimlik avı (phishing), omuz sörfü (shoulder surfing), tersine sosyal mühendislik (reverse social engineering) ve subaşı (waterholing)'dır (Şekil 1). Bu vektörlerin yanı sıra; bahane üretme (pretexting), taviz (quid pro quo), zıpkınla avlama (spear phishing), kuyrukçuluk (tailgaiting) gibi başka bileşenler de bulunmaktadır.

Kişisel veya kurumsal bilgilere yönelik günlük saldırılar birden fazla biçimde olabilirken, kullanıcılar tarafından benimsenen koruma düzeyi çoğu antivirüs veya güvenlik duvarı çözümünden ibaret olup, bu önlemlerin yeterli olacağına inanılmaktadır (Şerban ve Şerban, 2014: 9). Bu yaklaşım; tehlikenin boyutunu bilmeme ya da kestirememe, bilgi yetersizliği, teknoloji okur-yazarı olmama, önemsememe (daha ziyade çalışılan kuruma yönelik), sorumluluk taşımama vb. oluşmaktadır.

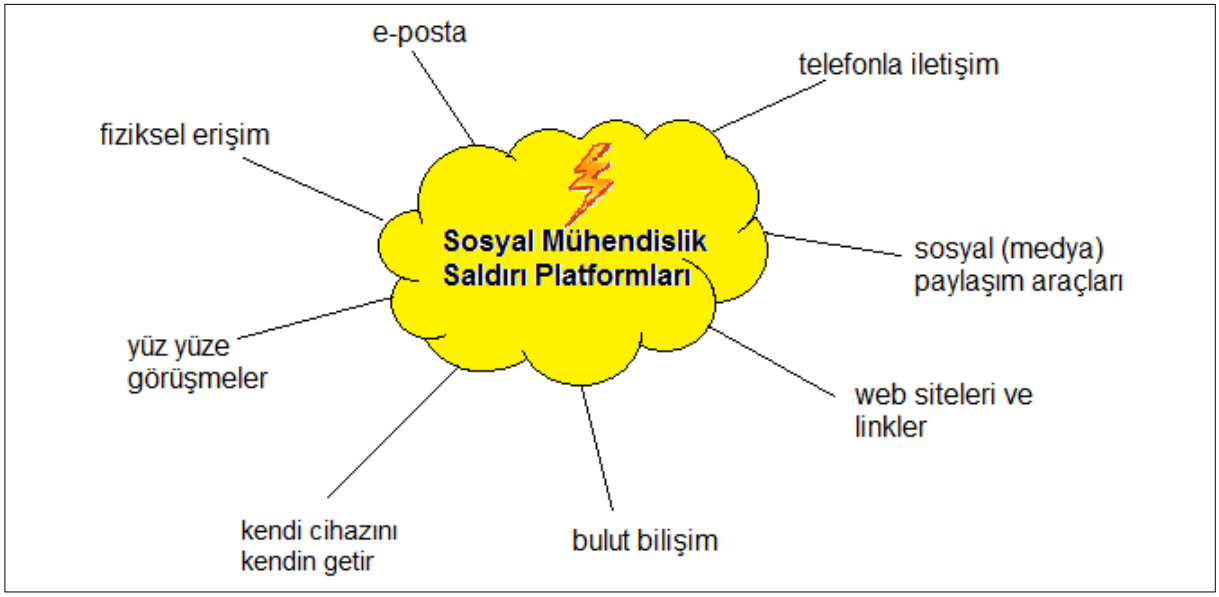


Şekil 1. Sosyal Mühendislik Saldırı Özellikleri ve Saldırı Senaryolarına Genel Bakış
Kaynak: Krombholz, Hobel, Huber ve Weippl (2014, s. 116)'den uyarlanmış ve geliştirilmiştir.

- ✓ **Çöp karıştırıcılığı** *(dumpster diving)*: Sosyal mühendis, kişi ya da şirketin çöp kutularını karıştırarak bazı değerli veri ya da bilgilere erişmek için çöp karıştırıcılığı yapar. Faturalar, isimler, müşteri bilgileri, kullanıcı adı ve parolalar, toplantı yerleri ve zamanları vb. onlarca bilgiye bu şekide erişmek olasıdır. Uygun şekilde imha edilmeyen bu bilgiler sosyal mühendise inanılmayacak sayıda ve çeşitte bilgi sunabilmektedir.
- ✓ **Gelişmiş kalıcı tehditler** *(advanced persistent threat)*: Bir sistemi kalıcı olarak oluşturma yeteneğine sahip bir saldırgan tarafından yürütülen uzun vadeli, çoğunlukla internet tabanlı casusluk saldırılarını ifade etmektedir (Krombholz vd., 2014:117).
- ✓ **Yemleme** *(baiting)*: Bir sosyal mühendis, kötü amaçlı yazılımları harici depolama aygıtlarına (CD, flash bellek vb.) önceden yükler ve stratejik olarak onları hedeflenen işin bulunduğu alana bırakır. Şüpheci yaklaşmayan çalışanlar, şirket bilgileri etiketli bu CD veya flash bellek'leri alır ve bilgisayarlarına takarlar. Bu şekilde zararlı yazılımlar kullanıcının bilgisayarına bulaşmış olur.
- ✓ **Kimlik avı** *(phishing)*: Sosyal mühendisler, kişilere yasal görünebilecek sahte e-postalar göndererek, kullanıcılardan bu e-postalarda yer alan kötü amaçlı bir bağlantıyı tıklamalarını talep eder. Bu şekilde çeşitli hassas bilgiler ele geçirilebilmektedir.
- ✓ **Omuz sörfü** *(shoulder surfing)*: Sosyal mühendisler, kurbanlarının kişisel bilgilerini almak için onlara hissettirmeden kullandıkları monitörlere, cep telefonlarına, diz üstü bilgisayarlarına, aldıkları notlara, çalışma alanlarındaki bilgi ve belgelere bakarlar. Bunun için en çok uygun alanlar; seyahat anları (yan ya da arka koltuk), banklar (yakın oturma), cafeler ve halka açık alanlar, çalışma alanları, toplantılar vb. dir.
- ✓ **Tersine sosyal mühendislik** *(reverse social engineering)*: Mağdurun (sözde) kendi isteği ile sosyal mühendisten yardım istemesidir. Örneğin; sosyal mühendis mağdurun bilgisayarını bozar ya da bozulmuş izlenimi yaratır. Daha öncesinden herhangi bir problemde her türlü yardıma hazır olduğunu bildiren sosyal mühendis bu sayede mağdurun yardım için arama listsinin en başında yer alır.

- ✓ **Subaşı** *(waterholing)*: Bu saldırı tipinde, sosyal mühendis seçilen kurbanın ilgisini çekebilecek bir ortamı (genellikle web sitesi) belirleyerek (tahmin ederek) pususunu oraya kurar ve kurbanının oraya giriş yapmasını bekler. Saldırı bu esnada gerçekleşir.
- ✓ **Bahane üretme** *(pretexting)*: Kötü niyetli saldırganlar, kişi veya şirket hakkında değerli bilgiler elde etmek için sahtekârlık yoluna başvururlar. Saldırgan, bir çalışanı arayarak, ondan (sözde) güvenlik amacıyla *kullanıcı adını* ve *parolasını* doğrulamasını ister.
- ✓ **Taviz** *(quid pro quo)*: Sosyal mühendis, mağduru zor bir durumdan kurtararak (kurtarmış gibi yaparak) onun şükranlarını kazanır. Bu şekilde mağduru kendisine borçlandırmış olur. İyiliğe iyilikle karşılık vermek isteyen mağdur artık sosyal mühendisin tuzağına düşmüştür.
- ✓ **Zıpkınla avlama** *(spear phishing)*: Kimlik avından farklı olarak hedef gözetilerek yapılan saldırıdır. Kime saldırılacağı önceden belirlenmiş ve spesifik hedef haline getirilmiştir.
- ✓ **Kuyrukçuluk** *(tailgaiting)*: Sosyal mühendis, belirli alanlara (korunaklı güvenli bölgelere, kartlı geçiş sağlanan alanlara, kontrollü geçiş noktalarına) erişim sağlamak maksadıyla, orada çalışan bir personelin peşine takılarak (gizli ya da sohbet ederek) erişimi kısıtlı olan alanlara girmeye çalışır.

Sosyal mühendislik saldırı platformlarına her geçen gün yeni bir yöntem eklenmekle birlikte en çok bilinenleri şu şekilde sınıflandırmak mümkündür: e-posta, telefonla iletişim, sosyal (medya) paylaşım araçları, web siteleri ve linkler, bulut bilişim, kendi cihazını kendin getir (bring your own device), ortalığa bırakılan cihazlar, yüz yüze görüşmeler ve fiziksel erişim (Şekil 2).



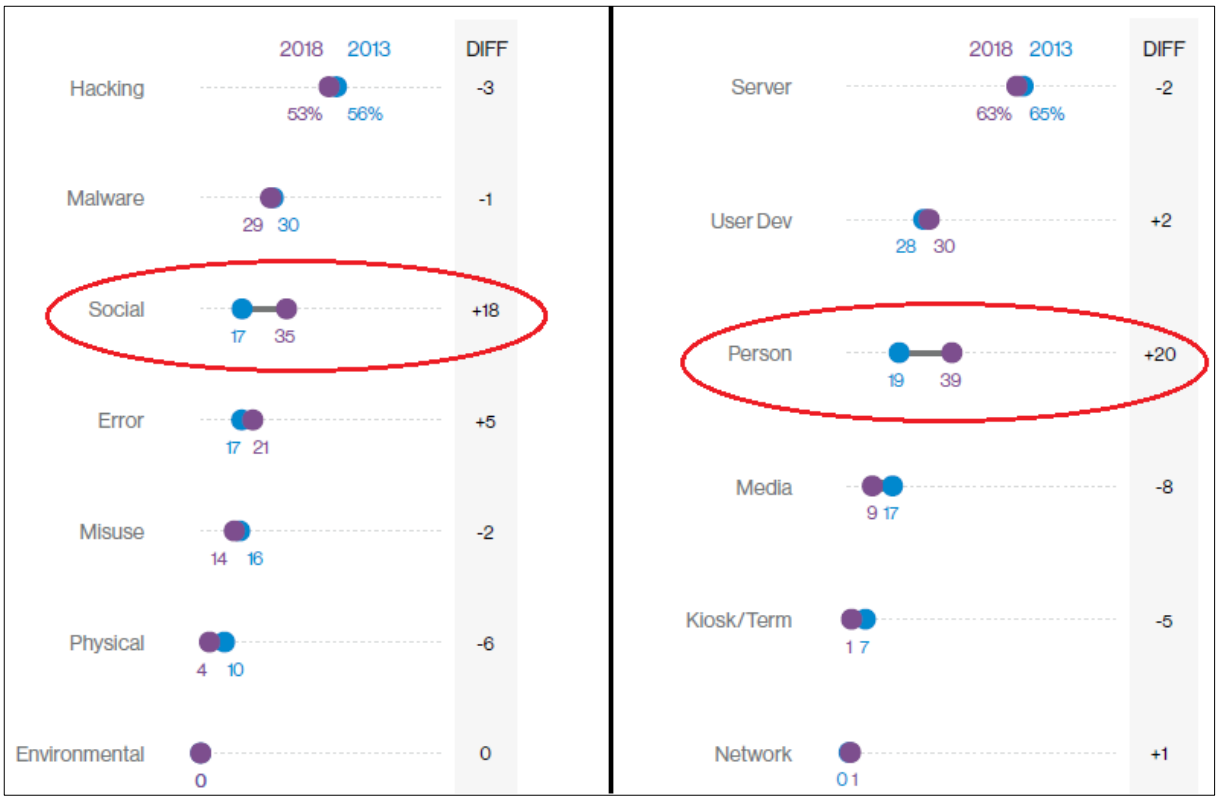
Şekil 2. Sosyal Mühendislik Saldırı Platformları

- ✓ **E-posta**: Sosyal mühendislik saldırılarında en çok kullanılan yöntemdir. Tekli ve çoklu hefedlere eş zamanlı yapılabilmektedir. Tehlikeli yazılımlar ve linkler içerir. Kurbanın bu yazılımları çalıştırması ya da linklere tıklaması özendirilerek saldırı gerçekleştirilir.
- ✓ **Telefonla iletişim**: Kullanıcıya ait kişisel bilgiler ya da iş yerine ait diğer bazı kıymetli bilgilerin (isim, telefon, kimlik bilgileri, sorumlu kişinin kim olduğu, hizmet sağlayıcı, iş [çözüm] ortaklarına ait bilgiler vs.) ele geçirilmesi maksatıyla telefon üzerinden kurban ile iletişime geçme yöntemidir. Saldırgan kendini genellikle önemli biri (üst yönetici, ya da resmi kurum çalışanı, emniyet görevlisi vb.) olarak tanıtarak bilgi edinmeye/karşısındakini yönlendirmeye çalışır. Tanıdık bir numaradan aramış gibi yapılarak da bu tür saldırılar düzenlenebilmektedir.
- ✓ **Yüz yüze görüşmeler**: Sosyal mühendisler, bazı bilgilere kolay ve hızlıca erişim sağlamak için yüz yüze görüşme yaparak, çeşitli psikolojik teknikler, vücut dili vs. kullanrak kurbanlarına

yaklaşmaya çalışırlar. Güven ortamı yaratıp, ortak konulardan bahsetme konusunda oldukça hünerli olan sosyal mühendisler, bu aşamadan sonra kurbanlarından bilgi devşirmeye başlarlar. Sosyal mühendisler genelde görüşme yapacağı kurban hakkında internet vb. platformlardan ön bilgi edinerek konuşmanın akışını önceden tayin etmek isterler.

- ✓ **Fiziksel erişim**: Erişime kısıtlı olan alanlara bir şekilde giriş yaparak çeşitli veri, bilgi ve kaynaklara erişim sağlama şeklinde gerçekleşir. *Tailgaiting* (kuyrukçuluk) bunlardan biridir. Kaba kuvvet kullanarak, zorla erişim (koruma, kilit ve vb. imha ederek) de söz konusudur. Bir diğer yöntem ise, çalışanlardan birisinin yaka kartını ele geçirerek giriş yapmak ya da üst yönetim tarafından yetkilendirildiğini söyleyerek giriş yapmayı denemek veya teknik ekip personeli gibi görünmeye çalışmak da söz konusudur.
- ✓ **Sosyal (**medya**) paylaşım araçları**: Bu tür platformlar hem bilgi toplamaya hem de toplanan bu ve diğer bilgilerin birleştirilerek kurbana yönelik olarak kullanılmasına fırsat tanımaktadır. Bu platformlarda yer alan bilgiler sanılandan daha fazla içerik sağlamaktadır (kimlerle birlikte olunduğu, zaman ve mekân, tercihler, kişisel görüşler, beğeniler, fotoğrafın nerede ve ne zaman çekildiği vs.). Ayrıca kurbanın tanıdığı ya da iletişimde olduğu kişilerin haritalanması açısından da çokça başvurulan bir mecradır.
- ✓ **Web siteleri ve linkler**: Daha çok *subaşı* (*waterholing*) ataklarında kullanılmaktadır. Zararlı yazılımlar içerebilen bu tür web siteleri ve linkler özellikle ilgi çekici kılınarak kurbanlar tuzağa düşürülmektedir. Kurbanın yaş grubuna göre de hazırlanabilen bu tür tuzaklarda saldırgan açısından başarı oldukça yüksektir. Örneğin; genç kuşaklar için daha çok ucuzluk içerdiği söylenen siteler, bedava pizza ve benzeri yiyecekler, ücretsiz gezi ve seyehatler, piyango ve çekilişler ilgi çekici olabilmektedir. Bu durumu bilen saldırgan ataklarını bu yönde geliştirmekte ve zenginleştirebilmektedir.
- ✓ **Bulut bilişim**: Ücretsiz alan sağlaması, virüs koruma vb. önlemlerinin yüksek olması, bedava yedekleme alanı sunması, bazen de bulut platform üzerinde çalıştırılan ve ücretsiz yararlanılabilen uygulamalar (aplikasyonlar) yüzünden kişisel ya da kurumsal veriler dışarıda (bulunulan mekânın dışında bir yerlerde) tutulabilmektedir. Öte yandan, kimin elinde olduğu, kimlerin erişebildiği ve güvenlik açısından ne durumda olduğu pek de belli olmayan bu tür platformlar veri/bilgi güvenliği açısından önemli açıklar yaratabilmektedir. Unutulmamalıdır ki bedava gibi gözüken hiçbir şey aslında bedava değildir.
- ✓ **Kendi cihazını kendin getir** *(bring your own device)*: Mesai saati uygulamayan ve çalışanlarından belirli saat diliminde belirli mekânlarda olmalarını şart koşmayan bazı şirketler, maliyeti de düşürmek amacıyla, çalışanların iş yerlerine kendi kişisel cihazlarını getirmesine izin vermektedir. Fakat içerisinde kötü niyetli yazılımların, virüslü programların olup olmadığı bilinmeyen bu cihazlar şirket ağına bağlandığında çeşitli güvenlik riskleri yaratabilmektedir.

İlginçtir ki, teknolojik yatırımlara ve bilgisayar güvenlik önlemlerine milyonlarca Dolar harcanırken, insan faktörü için benzer harcamaların yapılmadığını görmekteyiz. Oysa bu durumu fark eden sosyal mühendisler, saldırılarının önemli bir kısmını en zayıf halka olarak gördüklerli insan faktörü üzerinden gerçekleştirmektedir. Verizon (2019) Veri İhlali Araştırma Raporlarına (Data Breach Investigations Report) göre; 2013 yılından 2018 yılına gelindikçe sosyal ataklardaki artış %17'den %35'lere çıkmış, "varlık" kategorisinde ise insan faktörü %19'lardan %39'lara yükselmiştir. Dikkat çeken diğer bir husus ise, artış farkının en yüksek olduğu kategoriler açık ara ile sosyal ataklar (+18) ve insan faktöründe (+20) bulunmaktadır (Şekil 3).



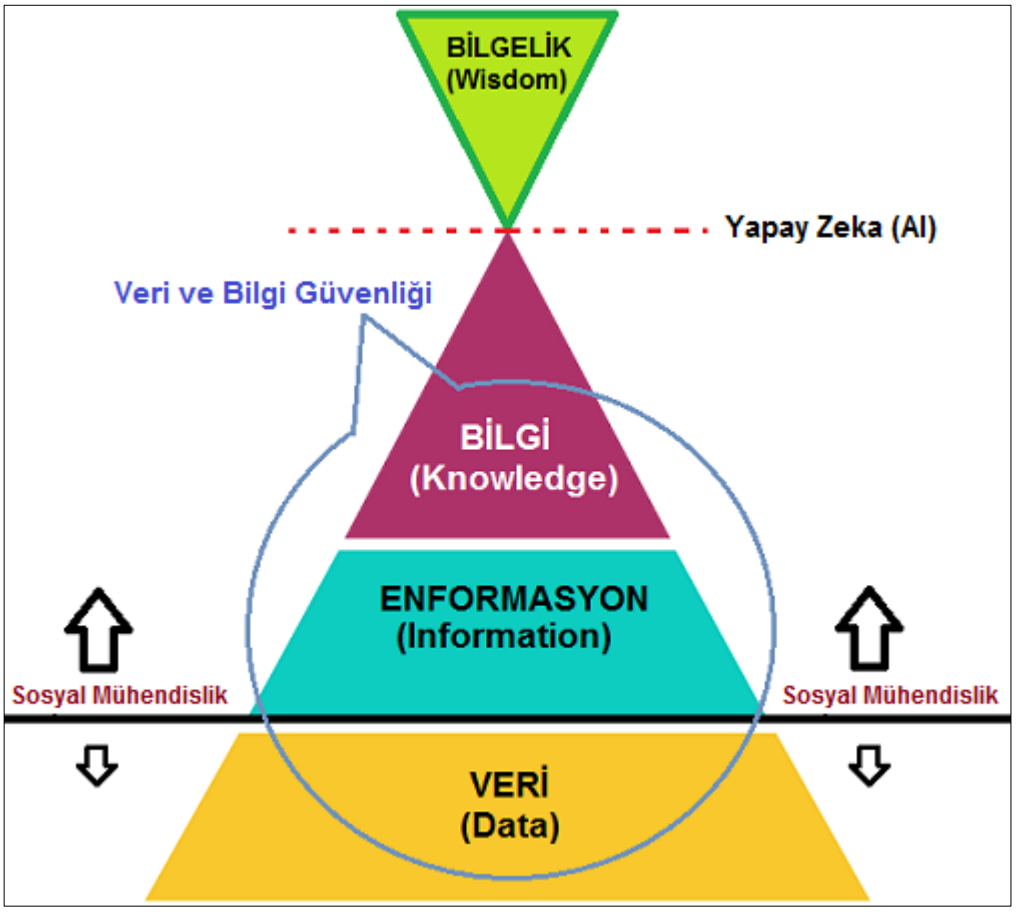
Zamana göre veri ihlallerinde tehdit eylemleri
n = 2.501 (2013), n = 1.638 (2018)

Veri ihlallerinde zamana göre "varlık" kategorileri
n = 2.294 (2013), n = 1.513 (2018)

Şekil 3. Veri İhlali Kategorileri
Kaynak: Verizon (2019) Data Breach Investigations Report

Dijitalleşen dünya, zaman ve mekândan bağımsız olarak hareket kabiliyeti kazandırmasının yanı sıra (doğru) bilgiye ulaşmak için yeni iletişim kanallarını insanlığın hizmetine sunmuştur. Bu iletişim kanalları arasında yolculuğuna devam eden bilgi, her yeni ekleme, çıkarma, dönüştürme, yeniden yorumlama işlemleri ile artık alındığı gibi kullanıl(a)mayan, ayıklanması gereken bir yapı kazanmıştır (Özdemir, 2015: 29).

Ackoff (1989)'un "veri-enformasyon-bilgi-bilgelik" hiyerarşik sınıflandırmasına dayanarak hazırlanan aşağıdaki şekilde (Şekil 4) görüleceği üzere sosyal mühendislik'in *veri*'ye doğru belirli ölçülerde etkili, *enformasyon* ve *bilgi*'ye yönelik ise daha fazla bir etki alanı geliştirdiğini düşünmekteyiz. Veri çokluğu, sosyal mühendislik müdahalelerine maruz kalan *enformasyon* ve *bilgi* alanları sonrasında yer alan *bilgelik* katmanına geçişlerin filtrelenmesi ve rafine edilebilmesi için bilgi ve bilgelik arasında yer almasını uygun gördüğümüz yapay zekâ uygulamalarına ihtiyaç duyulduğunu/duyulacağını düşünmekteyiz. Burada yer alan bilgelik alanı aynı zamanda arşiv ve kurum hafızasını da temsil etmektedir. Bu alana damıtılacak olan bilgilerin yapay zekâ ile (Şekil 4'te kesik çizgiler ile işaretlenmiş) aynı düzlemde eş zamanlı ve eş güdümlü olarak çalışacak doğrulama kaynaklarına (referanslara) ihtiyaç duyulduğunu da ifade etmek gerekir. Bu doğrulama kaynaklarının *merkezi olmayan* ve *dağıtık* bir yapı ile sağlanması ise güvenlik düzeyinin arttırılabilmesi açısından faydalı olacaktır.



Şekil 4. Veri-Enformasyon-Bilgi-Bilgelik Piramidinde Sosyal Mühendislik'in Etki Alanı
Kaynak: Ackoff (1989)'den uyarlanmış ve geliştirilmiştir.

5. SONUÇ

Sosyal mühendislik saldırılarından korunmak için en başta üst yönetimin üzerinde hassasiyetle durması gereken güvenlik politikalarınının oluşturulması ve uygulanması konuları yer almaktadır. Çalışanları sosyal mühendislik konularında bilgilendirmek, düzenli aralıklarla eğitim vermek ve çeşitli testler ile sınayarak eksiklerini görmek ise diğer önemli önlemlerin başında yer almaktadır. Yöneticiler, çalışanlardan parolalarını düzenli aralıklarla yenilemelerini talep etmelidir. Şirket dışından gelen ziyaretçilere, görüşeceği kişiye kadar görevli personelce eşlik edilmelidir. Şüpheli linklere tıklanmamalı, telefon görüşmelerinde ise gerçek kişilerin kimlikleri doğrulanmalıdır. Önemli veri ve bilgilerin tutulduğu alanlara erişim kontrollü sağlanmalı, içeriye ses ve kayıt cihazları vb. ile girişler yasaklanmalıdır. Teknolojik güvenlik önlemleri ise (anti-virüs programları, güvenlik duvarları, erken uyarı sistemleri, VPN ve kısıtlı IP erişim uygulamaları vs.) her zaman güncel olmalıdır. Tüm bu temel önlemlerin yanı sıra çeşitli zamanlarda profesyonel yardım alınarak *penetrasyon (sızma) test*'ler icra edilmeli ve sonuçlar açıklıkla rapor edilerek çalışanlar ve yöneticilere geri bildirimde bulunulmalıdır. Güvenlik önlemlerine tam olarak uyan çalışanlar ise çeşitli şekillerde ödüllendirilmelidir.

Güvenliğin gerektiği gibi sağlanabilmesi her şeyden önce *iş sürekliliği* için gereklidir. Bunun yanı sıra kârlılık ve sosyal sorumlulukların sürdürülebilmesi anlamına da gelebilmektedir. Bu ve benzeri birçok sebepten ötürü iş sürekliliği işletmeler açısından hayati öneme sahiptir. Bilgi güvenliği açısından sosyal mühendislik'e yönelik eğitimler her ne kadar tek başına yeterli olmasa da en kestirme ve en ekonomik güvenlik önlemlerinin başında yer almaktadır. Sosyal mühendislik'e yönelik alınabilecek önlemler, bilgi güvenliğine yönelik alınması gereken en kapsamlı koruma duvarının oluşturulabilmesinde ilk bakılması gereken yerlerin başında gelmelidir. Bu yaklaşımın her zaman göz önünde bulundurulması kurum ve devletlerin daima lehine olacaktır.

KAYNAKÇA

ACKOFF, R. L. (1989). From Data to Wisdo, *Journal of Applied Systems Analysis* (16), s.3-9.

AHSAN, S. ve SHAH, A. (2006). Data, Information, Knowledge, Wisdom: A Doubly Linked Chain? Research and Development Center of Computer Science. University of Engineering and Technology, Lahore

https://pdfs.semanticscholar.org/24b2/e7863c47f2e40071cd61faab1194941011d0.pdf (Erişim: 01.06.2020).

BAKTIR, H. Ö. (2013). Bilgi Paylaşım Ortamı Olarak Bilgisayar. Gülseçen, S. (Der.), *Bilgi ve Bilginin Yönetimi* içinde (s. 97-144). İstanbul: Papatya.

CONTEH, N. Y. (2016). The Dynamics of Social Engineering and Cybercrime in the Digital Age. *IRACST-International Journal of Computer Science and Information Technology & Security* (IJCSITS), ISSN: 2249-9555 Vol.6, No1, Jan-Feb 2016.

ÇUBUKÇU, F. (2018). Bilgi Güvenliği Yönetim Sistemi: ISO 27001:2013 Uygulama Kılavuzu. İstanbul: Pusula.

ISO (2016). International Organisation for Standardisation. Information Technology-Security Techniques-Information Security Management Systems-Overview and Vocabulary. ISO/IEC 27000:2016. Fourth Edition, 15 February 2016.

KARA, M. (2018). Kurumsal Bilgi Güvenliği: Yönetimsel ve Teknik Yönleriyle. İstanbul: Papatya Bilim.

KESER, H. ve GÜLDÜREN, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. *K. Ü. Kastamonu Eğitim Dergisi, 23 (3), 1167-1184.*

KROMBHOLZ, K., HOBEL, H., HUBER, M., WEIPPL, E. (2014). Advanced social engineering attacks. *Elsevier, ScienceDirect, Journal of Information Security and Applications*, (22), 113-122.

MOUTON, F., MALAN, M. M., KIMPPA, K. K., VENTER, H. S. (2015). Necessity for ethics in social engineering research. *Elsevier, ScienceDirect, Computer & Security* (55), 114-127.

OK, K. (2013). Bilgi ve Bilgi Yönetimine Giriş. Gülseçen, S. (Der.), *Bilgi ve Bilginin Yönetimi* içinde (s. 19-36). İstanbul: Papatya.

ÖZDEMİR, Ş. (2015). Aşırı Bilgi Artışı. Gülseçen, S. (Der.), *Bilgi Yönetimi: Bilgi Türeticileri, Büyük Veri, İnovasyon ve Kurumsal Zekâ* içinde (s. 29-38). İstanbul: Papatya.

PESEN, M. M. (06 Ağustos 2015). Bilgi Güvenliği Nedir ve Nasıl Sınıflandırılır.

http://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir/ (Erişim: 02.06.2020).

ŞERBAN, V. G. ve ŞERBAN, O. (2014). Social Engineering a General Approach. *Informatica Economică*, 18(2), 5-14. DOI: 10.12948/issn14531305/18.2.2014.01

UĞRAŞ, T. (2015). Bilgi Tüketicileri ve Üreticileri. Gülseçen, S. (Der.), *Bilgi Yönetimi: Bilgi Türeticileri, Büyük Veri, İnovasyon ve Kurumsal Zekâ* içinde (s. 17-28). İstanbul: Papatya.

VERİZON (2019). 2019 Data Breach Investigations Report.

YALÇINKAYA, İ. (2013). Bilgi Yönetiminin Örgütsel Etkileri. Gülseçen, S. (Der.), *Bilgi ve Bilginin Yönetimi* içinde (s. 37-49). İstanbul: Papatya.

YAZICIOĞLU, O., BORAT, O., KILIÇ, C. H. (2014). Bilgi Yönetimi. Ankara: Nobel.

YİĞİTBAŞI, İ. (2015). Bilginin Korunması. Gülseçen, S. (Der.), *Bilgi Yönetimi: Bilgi Türeticileri, Büyük Veri, İnovasyon ve Kurumsal Zekâ* içinde (s. 57-78). İstanbul: Papatya.

https://Kpssnotlar.com, Analitik Yaklaşım (08 Ocak 2017).

https://kpssnotlar.com/Default.aspx?ad=kpss_bilgi_detay&bilgi_id=5986 (Erişim: 13.06.2020).