TURKSOSBİLDER
Uluslararası Türk Kültür Coğrafyasında Sosyal Bilimler Dergisi

ÇAĞRI MERKEZİ ÇALIŞANLARININ ÇAĞRI MERKEZİ TEKNOLOJİLERİ VE SİBER SALDIRI-TEHDİT FARKINDALIKLARI

Dr. Sami ACAR, Gazi Üniversitesi, samiacar@gazi.edu.tr
Dr. Selin AYGEN ZETTER, Akdeniz Üniversitesi, selinaygen@akdeniz.edu.tr
Dr. Nuran ÖZTÜRK BAŞPINAR, Anadolu Üniversitesi, nbozturk@anadolu.edu.tr

ÖZET

Araştırmanın temel amacı, çağrı merkezi çalışanlarının çağrı merkezi teknolojileri ve siber saldırı-tehdit farkındalıklarını ortaya koymaktadır. Bu amaç doğrultusunda araştırma, nicel verilere dayalı tarama araştırması olarak tek grup tek ölçüm (anlık) şeklinde desenlenmiştir. Araştırmanın çalışma grubunu, Antalya bölgesindeki çağrı merkezlerinde çalışan 48 çağrı merkezi çalışanı oluşturmaktadır. Araştırmada veriler, "Çağrı Merkezi Teknolojileri ve Siber Saldırı-Tehdit Farkındalığı (ÇMTSSTF)" ölçeği ile elde edilmiştir (α=0,92). Ölçekte, çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalığı boyutuna ilişkin 8 madde (α=0,85), siber saldırı-tehdit farkındalığı boyutuna ilişkin 8 madde (α=0,90) yer almıştır.

Araştırmada ÇMTTSSTF ölçeği ile elde edilen veriler, bilgisayar ortamında SPSS istatistiksel analiz programı ile analiz edilmiş ve elde edilen bulgular ışığında çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalıklarının orta düzeyde, siber-saldırı tehdit teknolojileri farkındalıklarının düşük düzeyde olduğu ve bu teknolojilere ilişkin farkındalıklarının demografik değişkenlere göre önemli bir farklılık göstermediği sonucuna varılmıştır. Araştırmaya ilgi duyan alan yazındaki araştırmacılara, daha fazla katılımcının bulunduğu farklı bölgelerdeki çağrı merkezlerinde ve farklı değişkenler boyutunda araştırmalar yapmaları önerilebilir.

Anahtar Kelimeler: Çağrı Merkezleri, Çağrı Merkezi Teknolojileri Farkındalığı, Siber Saldırı-Tehdit Farkındalığı

ABSTRACT

Call Center Technologies And Cyber Attack-Threat Awarenesses Of Call Center Employees

The main aim of this research is to reveal call center technologies and cyber attack-threat awarenesses of call center employees. In accordance with this purpose, the research designed as a quantative survey research based on quantative data. The study group of the research is constituted of 48 call center employees working in the province of Antalya. The data in the study is obtained with scale of "Call Center Technologies and Cyber Attack-Threat Aweranesses (CCTCATA)" (α=0,92). In the scale, there are 8 items related to call center technologies awareness (α=0,85) and 8 items related to cyber attack-threat awareness (α=0,90) of call center employees.

In this research, the data obtained with scale of CCTCATA was analyzed in SPSS statistical analysis program, and in the light of the research findings, it is concluded that call center technologies awareness of call center employees is at a medium-level, cyber attack-threat technologies awareness is at a low level, and there is no significant difference according to demographic variables related to these technologies. Researchers who are interested in research can be encouraged to conduct similar studies in other regions call centers where more participants are located, and in different variables.

Keywords: Call Centers, Call Center Technologies' Awareness, Cyber Attack-Threat Awareness

SUMMARY

The main aim of this research is to reveal call center technologies and cyber attack-threat awarenesses of call center employees. In accordance with this purpose, the research designed as a quantative survey research based on quantative data. The study group of the research is constituted of 48 call center employees working in the province of Antalya. The data in the study is obtained with scale of "Call Center Technologies and Cyber Attack-Threat Aweranesses (CCTCATA)" (α=0,92). In the scale, there are 8 items related to call center technologies awareness (α=0,85) and 8 items related to cyber attack-threat awareness (α=0,90) of call center employees.

As a result of the analysis of the data obtained with scale of CCTCATA, it has been reached that most of participants were women (%58,3), the age interval is mostly 25-30 years (%35,4), the year worked at the call center is mostly within 1-5 years (%70,8), the position in the call center more than half of employees are call receiver(%66,7). In addition to this findings, it is observed that most of participants (%83,3) are heard the term of cyber threat before; however, the number of trainees about this topic are quite few (%16,7); similarly, most of participants (%66,7) are heard the term of call center systems security; yet, the rate of trainees educated this topic are very low (%18,8). It was found that call listening and response systems, internet and network connection, and compture hardware awarenesses of call center technologies of call center employees are at a high level; firewall and communication tools software awarenesses are at a low level. It was observed that harrasing callers and robo-calling scams, voice phishing and spam awarenesses of cyber attack-threat are at a high level; social telephony denial of service (tDos) attacks, SIP packet/network level attacks and modem/ISP calls-fax abuse awareness are at low level. Furthermore, in this research, it was found that call center technologies awareness of call center employees is at a medium-level ($\bar{x}$=3,13), and cyber attack-threat technologies awareness is at a low level ($\bar{x}$=2,36). Call center technologies and cyber attack-threat awarenesses of call center employees were examined according to demographic variables such as gender, age, worked year and position at call center, there was no significant difference according to these variables.

In the light of the research findings, we can say that call center technologies awareness of call center employees is at a medium-level, cyber attack-threat technologies awareness is at a low level, and there is no significant difference according to demographic variables related to these technologies. Researchers who are interested in research can be encouraged to conduct similar studies in other regions call centers where more participants are located, and in different variables.

Keywords: Call Centers, Call Center Technologies' Awareness, Cyber Attack-Threat Awareness

1- Giriş

Küreselleşme ve gelişen teknoloji ile birlikte sürekli değişim ve inovasyonun sonucunda işletmelerin rekabet ortamında rakiplerinin bir adım önde olma isteği farklı rekabet stratejileri kullanma isteği ve zorunluluğunu da arttırmıştır. Yeni arayışlar yeni teknolojileri, yeni çalışma modelleri ve stratejilerini de beraberinde getirmiştir. Özellikle, 1980'li yıllardan itibaren bilgi ve iletişim teknolojisindeki gelişmelerle birlikte hizmet sektörünün dış kaynak kullanımının yaygınlaşmasının sonucu oluşan üretici hizmetlerden biri olarak çağrı merkezleri bu platformda yerini almaya başlamıştır (Seçkin & Ökten, 2009, s. 193; Taşkın & Taşkın, 2018) Çağrı merkezlerinde kullanılan teknolojiler bilgi çağında ve içinde bulunduğumuz bilgi yoğun rekabet ortamında sürekli değişmekte ve gelişmektedir. Çağrı merkezlerinin yoğun olarak kullanılmaya başlamasıyla birlikte rakip sayısı da hızla artmış ve organizasyonlar ile müşterileri arasında iletişim araçlarının doğru kullanımı da önemli olmaya başlamıştır (Sarıyer, 2007, s. 473).

Çağrı merkezleri, mevcut teknolojiler üzerine kurulan interaktif sesli yanıt teknolojisine ve otomatik çağrı dağıtım sistemine de sahiptir (Robinson & Morley, 2006, s. 284).

Alanyazın incelendiğinde çağrı merkezleri (Holman vd, 2002; Gans vd., 2003; Dean, 2004; Brown vd., 2005), çağrı merkezi teknolojileri (Bernett & Jaramillo, 2001; Aksin vd., 2007), siber saldırı-tehdit (Cohen, 1999; Lala & Panda, 2001), teknoloji farkındalığı (Baptista vd., 2010) ve siber saldırı-tehdit farkındalığı (Dutt vd., 2003) üzerine bir çok çalışmanın yapıldığı, fakat çağrı merkezinde çalışanların çağrı merkezi teknolojileri farkındalıkları ile siber saldırı-tehdit farkındalıklarını ele alan bir çalışmanın bulunmadığı görülmüştür. Bu nedenle araştırmanın problem cümlesi; "çağrı merkezi çalışanlarının çağrı merkezi teknolojileri ve siber saldırı-tehdit farkındalıkları nedir?" şeklinde belirlenmiştir..

2. Çağrı Merkezlerinde Kullanılan Teknolojiler

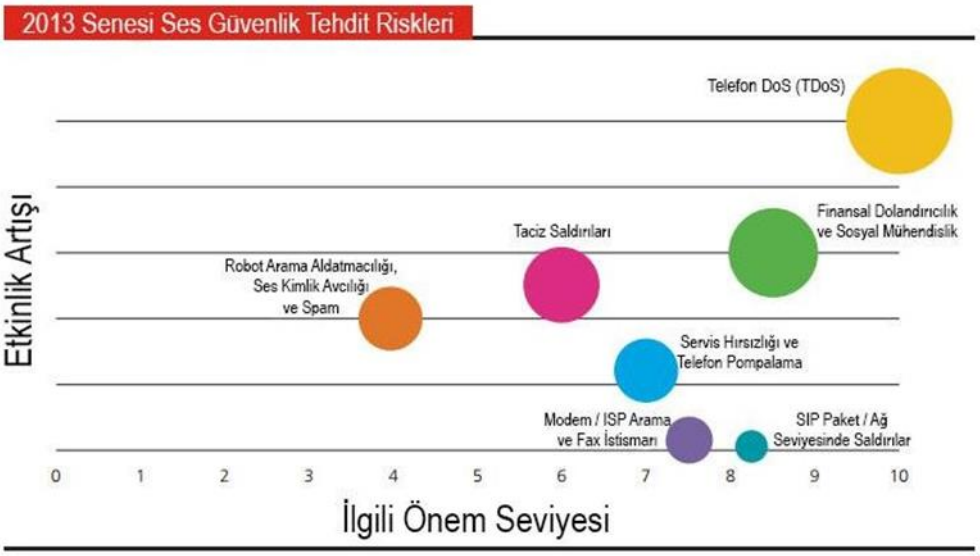
Çağrı merkezlerinde kullanılan teknolojiler, donanım ve yazılım olarak bütünleşik ve bağlantılı bir yapıdadır. Çağrı merkezlerindeki müşteri ve işletme arasındaki iletişimin sağlanabilmesi için kullanılan bu teknolojileri şu şekilde sıralanabilir:

- ✓ İnternet bağlantısı,
- ✓ VoIP hattı (IP telefon numarasıdır. Küçük kuruluşlar bunu kontör gibi ödeme seçenekleriyle kiralayabilirken, büyük firmalar sabit tarifelerle çalışmaktadırlar),
- ✓ Kulaklık ve mikrofon,
- ✓ Çağrı merkezi santral yazılımları,
- ✓ Softphone çevirici yazılımları (bilgisayar üzerinden arama yapmaya yardımcı yazılımlardır),
- ✓ Müşteri takip ve destek yazılımları ve tüm bu süreçlerin üzerinde yürütüleceği bilgisayarlar.

Çağrı merkezlerindeki kullanılan bu teknolojiler ile müşterilerine dünyanın her tarafından aynı mesafedeymişçesine ulaşabilen işletmeler, çağrı merkezlerinin kapasite ve isteklerine göre çeşitli sistemler entegre edebilmektedirler. Ancak kullanılan tüm bu teknolojiler, her geçen gün farklı güvenlik problemlerini de beraberlerinde getirmektedirler.

3. Çağrı Merkezleri Teknolojilerine Yönelik Siber Saldırılar, Tehditler ve Alınabilecek Önlemler

Dolandırıcılar ve organize suç örgütleri, iletişim sistemlerinin zayıf noktalarını tespit ederek buldukları bu zafiyetleri kendi çıkarları adına kullanmaktadırlar. Her geçen gün farklı tehditler ortaya çıkmakta ve bu tehditlerin yol açabileceği riskler artmaktadır. Bilgisayar korsanlarının önemli bir kısmının çağrı merkezlerine yapmış olduğu saldırı türleri incelendiğinde; çağrı merkezlerinin santralleri ile hedef kitlenin iletişimini kesmeye odaklı olduğu görülmektedir. 2013 senesi ses güvenlik tehdit riskleri incelendiğinde; telefon DoS (TDoS)' un en yüksek önem seviyesine sahip olan saldırı-tehditi olduğu görülmektedir (Şekil-1).



Şekil-1: 2013 Senesi Ses Güvenlik Tehdit Riskleri (Kaynak (Voice & Unified Communications , 2014)

SecureLogix Voice & Unified Communications tarafından State of Security Report 2014'de belirtilen tehditler ve bu tehditlere yönelik çözüm önerileri bu araştırmada detaylı olarak sunulmuştur. Modem/ISP arama, faks istismarına ve SIP paket/ağ seviyesindeki saldırılara önem seviyesinin düşük olması ve çözüm önerilerine yönelik hali hazırda çalışmalar bulunması sebebiyle yer verilmemiştir.

3.1. Telefon DoS (TDoS)

Asıl hedefi çağrı merkezleri olan TDoS saldırıları, dünya çapındaki tüm çağrı merkezlerinin en önemli siber güvenlik tehditleri arasında yer almaya başlamıştır. Şekil-1'de 2013 senesi ses güvenlik tehdit riskleri incelendiğinde Telefon DoS saldırıların önem seviyesinin ve etkinlik artışının zirvede olduğu görülmektedir. Bunun en önemli sebebi ise etkili bir saldırı yöntemi olması ve saldırganların eylemlerini başarıyla tamamlama oranlarının yüksek olmasıdır.

Bir DoS türevi olan TDoS saldırıları (Telephony Denial of Service Attack), hedef sistemin kaynaklarını veya bant genişliğini istilaya uğratarak hizmetlerini sağlayamaz duruma getirme işlemidir. Telefon DoS saldırılarını düzenleyen bilgisayar korsanlarının saldırı motivasyonu, DoS ve DDoS saldırı motivasyonları ile benzerlikler göstermektedir. Temel olarak saldırganların motivasyonları incelendiğinde:

- ✓ Firmalardan çıkar elde etme,
- ✓ Rakip firmaya zarar verme,
- ✓ Hactivism (siber farkındalık veya toplumsal mesajlar bırakmak amacıyla yapılan eylemler) gibi nedenler ortaya çıkmaktadır.

Bu tür saldırılar genellikle sistemlerin yoğun olarak kullanıldığı vakitlerde yapılır. Bu saldırılar birçok farklı araç kullanılarak yapılabilmektedir. Telefon DoS saldırıları:

- ✓ Asterisk ve benzeri SIP sunucular,
- ✓ Bilgisayarlar üzerine kurulan SIP uygulamaları,
- ✓ Mobil/PSTN telefon hatları gibi araçlarla yapılabilmektedir.

Bu saldırı türüyle:

- ✓ Çağrı merkezlerindeki yönlendirici ve yönetici yazılımsal ajanların tutulabildiği kadar uzun süre telefon hatlarında tutulması sağlanarak hem çağrı merkezi iletişim altyapısının hem de insan kaynaklarının tüketilmesi amaçlanabilir.

- ✓ TDoS saldırıları aracılığıyla kesilen çağrı merkezi hattı, Man in the Middle (MIDM-ortadaki adam) saldırı tekniği kullanılarak bilgisayar korsanlarınca firmanın telefon trafiği kontrol edilebilir ve firma dışındaki kötü niyetli kişilerce telefonlara yanıt verilebilir. Bu yolla firmaların toplumsal imajı zedelenebilir. Man in the Middle tekniğinde temel olarak mantık, sunucu ile kurban arasına girerek maskeleme yapmaktır.

  Telefon DoS saldırıları ile firmalara telafisinin mümkün olamayacağı büyüklükte zararlar verilebilmektedir.

  Telefon DoS saldırıları diğer saldırı yöntemlerine göre tespit edilmesi kolay bir saldırı yöntemidir. Bir çağrı merkezi çalışanı durumlarda:

- ✓ Sistem her zamankinden yavaş çalışmaya başlamış ise,
- ✓ Konuşma esnasında tüm çalışanların seslerinde kopmalar başlamış ve kaliteli iletişim sağlanamıyor ise,
- ✓ Telefon konuşmaları sırasında hat'a farklı kişiler bağlanıyor ve olağan dışı sesler duyuluyorsa organizasyonlarındaki bilişim güvenlik uzmanlarına bilgi vermelidir.
- ✓ Teknik bir çalışanın, telefon DoS saldırısı olup olmadığını anlayabilmesi için ağ analizi yapması gerekmektedir. Bu ağ analizinde normalden fazla kaynak veya ağ kullanımı söz konusu ise gelmekte olan istekler önlenmeli veya filtrelenmelidir.
- ✓ Bir çağrı merkezinin kapasitesinin üzerinde isteklerde bulunularak, çağrı merkezinin hizmet veremez haline getirilmesi esasına dayalı telefon DoS saldırılarını teknolojik cihazlar ve yazılımlar aracılığıyla bir yere kadar önleyebilmek mümkündür. Bunun için firewall ve IPS gibi sistemler kurulabilmektedir. Fakat gelen herhangi bir telefon DoS saldırısı durumunda bilişim güvenlik uzmanlarınca bu saldırgan/saldırganların trafiklerinin erişimleri engellenmelidir.

3.2. Finansal dolandırıcılık ve sosyal mühendislik

Finansal dolandırıcılık ve sosyal mühendislik; iletişim teknolojilerinin gelişmesi ve kullanım oranının artmasına paralel olarak gün geçtikçe artmaktadır. Çağrı merkezlerinde kullanılan bu yöntemlerle kişilerin internetteki zafiyetlerinden faydalanılarak istenilen bilgilerin elde edilmeye çalışıldığı görülmektedir. Sosyal mühendisler, sosyal ilişkiler kurarak, sistemin açıklarından yararlanıp bilgi toplayarak bu dolandırıcılığı gerçekleştirmektedir. Bu açıklar sanıldığı gibi sistemsel açıklar değildir. Kişileri ikna yöntemiyle kişisel bilgilerine ulaşma şeklindedir. Böylece kişilere sezdirilmeden şifre ve güvenlik tedbirleriyle ilgili bilgi almaya çalışılmaktadır. Sosyal mühendislik dolandırıcılığı daha çok senaryolar üzerine oturtulmuş ve genellikle dolandırıcıların kendilerini çağrı merkezi tarafından arayan bir personelmiş gibi tanıtarak, kişilerden şifre gibi özel bilgilerinin sızdırılması şeklinde gerçekleştirilmektedir (Açıkgöz, 2016, s. 399).

Bilgisayar korsanlarının son zamanlarda finansal dolandırıcılık suç faaliyetleri için bankaların online sistemleri yerine çağrı merkezlerinin telefon santrallerini hedef aldığı gözlemlenmektedir. Çünkü saldırganların yakalanma riskleri düşük ve başarılı olma ihtimalleri ise yüksektir. Günümüzde bankalarda güvenlik görevlileri, kasalar, gelişmiş takip sistemleri, kameralar vb. birçok fiziksel ve çevresel güvenlik önlemi olduğundan birebir bu tip bir işi yapmak hem tehlikeli hem de çok risklidir. Benzer şekilde birçok bilişim güvenliği firmasıyla çalışmakta olan bankaların web sistemlerine veya veri tabanlarına yapılan saldırıların da başarılı olma ihtimali çok düşüktür.

Çağrı merkezi çalışanlarınca finansal dolandırıcılık ve sosyal mühendislik tehditlerinin riskinin farkında olunarak, işletme kurallarının ve güvenlik politikalarının her zaman göz önünde bulundurulması ve arayan kişilere uygulanması bir nevi caydırıcı etkiye sahiptir. Çağrı merkezi çalışanının böyle bir durumla karşılaşması veya tedirgin olması durumunda, olayı çağrı merkezi sorumlusu üstlerine bildirmeleri gerekmektedir.

3.3. Servis hırsızlığı ve telefon pompalama

Bu saldırı tipi genellikle Sesli Yanıt Sistemi (IVR: Interactive Voice Response) bulunan ve ücretsiz aramaların yapılabildiği çağrı merkezlerine yöneliktir. Bilgisayar korsanları tarafından geliştirilen uygulamalar aracılığı ile çağrı merkezlerindeki sesli yanıt sisteminin olabildiğince uzun süre aktif olarak çalışması sağlanmaktadır. Böylece hattın sahibi kurum veya kuruluşun faturaları kabartılmakta ve hizmet vermesi engellenmektedir.

Bilgisayar korsanlarınca yeni bir saldırı yöntemi ise servis hırsızlığı yöntemidir. Servis hırsızlığı yöntemi ile santral veya SIP sunucu hizmetlerine sızılarak tanımlanan hat aracılığıyla sistemin kaynakları kullanılmaktadır. Bu yöntem sonucunda, yetkili bilişim uzmanları tarafından fark edilene kadar sistem kaynakları suç örgütlerinin çıkarları için hizmet vermeye devam etmektedir.

Servis hırsızlığı ve telefon pompalama tehditlerinin tespiti kolay olmamaktadır. Bunun en büyük sebebi ise servis hırsızlığı yönteminde sistem kaynaklarının işletmenin haberi olmayacak şekilde kullanılmaya çalışılmasıdır. Bu durumun tespiti için teknik personelin dikkatli olması ve düzenli olarak sistemlerin kontrolünü sağlaması ve aynı zamanda bilişim güvenlik uzmanlarının da periyodik olarak güvenlik kontrollerini yapması gerekmektedir. Bu saldırı türlerinde arayan müşterilerin yorumları ve uyarıları var ise kesinlikle dikkat edilmelidir. Örneğin; arayan bir müşteri "… tarafıma sizin numaranızdan arama yapılmış" şeklinde bir geri dönüt sağladığında, böyle bir aramanın firma tarafından yapılmadığına emin olan bir çalışanın durumu çağrı merkezi sorumlusuna bildirmesi gerekmektedir.

3.4. Taciz Saldırıları

Taciz aramaları aslında ses alanında yeni bir saldırı yöntemi değildir. Fakat son yıllarda giderek artış göstermeye başlamıştır. Taciz aramaları, TDoS, dolandırıcılık, tele-satış (telemarketing), tanıtım, korkutma, propaganda vb. saldırı tiplerini de kapsamaktadır. Bu saldırı tipi son yıllarda kurumsal işletmeler için büyük bir sorun olarak görülmeye başlanmıştır. Taciz aramaları memnuniyetsiz müşterilerin ve eski çalışanların intikam almak için, pazardaki rakip firmaların ise itibar kaybettirmek ve hizmet kesintisi yaratmak için başvurdukları en ucuz yöntemdir. Fake Caller (Fake Caller ID vb. uygulamalar) uygulamaları ile yapılabilen bu saldırıların tercih edilme sebepleri arasında:

- ✓ Güvenli olması,
- ✓ Herhangi bir maddi külfete yol açmaması,
- ✓ Amacına ulaşmada etkili sonuçlar doğurması yer almaktadır.

Taciz saldırıları genelde müşterinin her koşulda haklı olduğunun kabul edilmesi, müşteri memnuniyeti gibi yoğun rekabet ortamında bu koşullardan yararlanmak için fırsat kollayan saldırganların bir firmadan istediği bir sonucu alamaması veya toplumsal eylemler sebebiyle gerçekleştirilmektedir (Boyd, 2002, s. 162).

Çağrı merkezi çalışanlarının böyle bir olay ile karşılaşması durumunda çağrı merkezi sorumlusuna durumu iletmesi gerekmektedir. Çağrı merkezi sorumlularının bu sorunun çözümüne yönelik çalışmalar yürütmesi gerekir. Ayrıca bot ve benzeri sistem aramalarını önlemek için kısa güvenlik soruları sordurma gibi yöntemlere başvurulması gerekir. Fakat bu durum müşterinin çağrı merkezine ulaşım kalitesini düşürmektedir (örneğin; 2+2=4 şeklinde arayan kişilere sorular yöneltilmesi, iletişime geçme süresini düşürmektedir).

3.5. Robot arama aldatmacılığı, ses kimlik avcılığı ve spam

Robot arama aldatmacılığı veya spam çağrılar daha çok banka çağrı merkezlerine yönelik olarak sahte isimler ve uydurma telefon numaraları aracılığıyla yapılan ve kuyrukta bekleyen müşteriler varmış gibi gösterilmek istenen saldırılardır. Ses kimlik avcılığı ile ise elde edilen telefon listesiyle kişilerden özel bilgiler istenmesi şeklinde gerçekleştirilmektedir. Bu istekler hali hazırda alınmış ve kendini banka olarak tanıtan ses kayıtlarıyla yapılmaktadır. Örneğin, kendisini bir çağrı merkezi gibi tanıtan bu sistemle kişilerden "görüşmenin güvenliği, kimliğin doğrulanması" gibi sebeplerle kart numarasını veya PIN kodunu girmesi istenmektedir.

Robot arama aldatmacılığı veya spam saldırı yöntemlerini kullanan kişiler genellikle hazır yazılımlar kullanmaktadırlar. Saldırganın amaçları:

- ✓ Kişi hakkında deneme yanılma yoluyla bilgiler edinmek (Örneğin; doğum tarihi ve kimlik numarasını eşleştirerek kişiye dair banka hesabındaki bakiyesini öğrenmek),
- ✓ Çağrı merkezini meşgul ederek sistemlerin kaynaklarını gereksiz yere tüketmek,
- ✓ Müşteri temsilcisine bağlanmayı bekleyen kişileri uzun süre kuyruklarda bekletmek ve işletmenin imajını zedelemek olabilmektedir (Kocabaş, 2017, s. 129).

Bu saldırıların tespitinde santral uygulamasının "sırada bekleyen müşteri" sayısının iyi analiz edilmesi gerekmektedir. Çağrı merkezi çalışanı her zamanki değerlerin üstünde rakamlar görmeye başladığında durumu çağrı merkezi sorumlusuna iletmelidir. Robot aramaların ve spam saldırılarının önlenmesi için müşterilere "2+2=4" gibi basit soruların yöneltilmesi ve yanlış cevap verilmesi durumunda santral tarafından otomatik olarak çağrının sonlandırılması gerekir.

Ses kimlik avcılığında ise durum farklıdır. Suç örgütleri kişilere ait özel (PIN kodu, banka kartı CVV kodu vb.) bilgilere ulaşarak bunları genellikle maddi gelir elde etmek amacıyla kullanırlar.

Çağrı merkezlerinin ses kimlik avcılığı saldırı durumlarından haberdar olması kolay olmamaktadır. Müşteri çağrıları bu saldırının tespiti için önemli bir yere sahiptir. Bu sebeple müşterilerin durumla ilgili beyanlarının dikkate alınması ve çağrı merkezi sorumlusuna bilgi verilmesi gerekir.

4. Amaç, Önem ve Sınırlılıklar

4.1. Amaç

Araştırmanın temel amacı, çağrı merkezi çalışanlarının çağrı merkezi teknolojileri ve siber saldırı-tehdit farkındalıklarını ortaya koymaktadır. Bu ana amaç doğrultusunda belirlenen alt amaçlar ise şu şekildedir:

1. Çağrı merkezi çalışanlarının cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyonuna ilişkin dağılımı nedir?
2. Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalık düzeyleri nedir?
3. Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalık düzeyleri nedir?
4. Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalıkları cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyona göre farklılık göstermekte midir?
5. Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalıkları çağrı merkezi sistemleri güvenliğini duyup duymama ve bu konuda eğitim alıp almama durumuna göre farklılık göstermekte midir?
6. Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalıkları cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyona göre farklılık göstermekte midir?
7. Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalıkları siber saldırı-tehdit kavramını duyup duymama ve bu konuda eğitim alıp almama durumuna göre farklılık göstermekte midir?

4.2. Önem

Çağrı merkezi teknolojileri her geçen gün biraz daha gelişmekle birlikte çalışanların farkındalık düzeyleri aynı paralellikte gelişmemektedir. Bu araştırma ile çalışanların siber saldırı-tehditlerine karşı farkındalık kazanmaları ve bu tür olaylarla karşılaştıklarında önlem almaları ile ilgili çözüm yolları üretebilmeleri için yol gösterici olması umulmaktadır.

4.3. Sınırlılıklar

Araştırma, Antalya bölgesinde hizmet veren çağrı merkezlerinde çalışanlar (çağrı alıcı ve çağrı yönlendirici olarak çalışanlar), bu kişilerden 1-15 Mart 2018 tarihinde veri toplama aracıyla (anket ile) elde edilen veriler ve bu verilere ilişkin elde edilen istatistiksel analizler sonucu elde edilen bulgular ile sınırlıdır.

5. Yöntem

5.1. Araştırma modeli

Araştırma, nicel verilere dayalı tarama araştırması olarak tek grup tek ölçüm (anlık) şeklinde desenlenmiştir.

5.2. Çalışma grubu

Araştırmanın çalışma grubunu, Antalya bölgesindeki 48 çağrı merkezinde çağrı alıcı ve çağrı yönlendirici gibi benzer konumlarda çalışan çağrı merkezi çalışanları oluşturmaktadır. Çalışma grubu belirlenirken, basit seçkisiz örnekleme yönteminden yararlanılmıştır.

5.3. Verilerin toplanması ve analizi

Araştırmada öncelikli olarak literatür araştırması yapılmış olup, literatür araştırması sonucunda elde edilen kuramsal çerçeve ışığında ve alandaki uzmanların görüşü de alınarak yazarlar tarafından geliştirilen ölçek (online anket formatında) kullanılarak çağrı merkezi çalışanlarının çağrı merkezi teknolojileri ve siber saldırı-tehdit farkındalıkları üzerindeki etkisi araştırılmıştır.

Araştırmada veriler, "Çağrı Merkezi Teknolojileri ve Siber Saldırı-Tehdit Farkındalığı (ÇMTSSTF)" ölçeği ile elde edilmiştir (α=0,92). Ölçekte, çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalığı boyutuna ilişkin 8 madde (α=0,85), siber saldırı-tehdit farkındalığı boyutuna ilişkin 8 madde (α=0,90) yer almıştır. Ölçekteki çağrı merkezi teknolojileri ile siber saldırı-tehdit teknolojileri arasında ilişki olup olmadığına ilişkin yapılan korelasyon analizine (Pearson r'ye) göre bu iki boyut arasında pozitif yönde anlamlı bir ilişkinin olduğu görülmüştür ($r=0,654$; $p<0,01$).

Araştırmanın amacı ve araştırma modeli çerçevesinde ÇMTSSTF ölçeği ile elde edilen veriler SPSS istatistiksel analiz programında analiz edilmiştir. Verilerin analizinde;

- Çağrı merkezi çalışanlarının cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyonuna ilişkin dağılımı için frekans ve yüzde istatistiklerinden,
- Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri ile ilgili farkındalık düzeylerini belirlemek için aritmetik ortalamadan,
- Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri ile ilgili farkındalık düzeylerini belirlemek için aritmetik ortalamadan,
- Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalıkları cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyona göre farklılık gösterip göstermediğini belirlemek için çok faktörlü varyans analizinden (MANOVA),
- Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalıkları çağrı merkezi sistemleri güvenliğini duyup duymama ve bu konuda eğitim alıp almama durumuna göre farklılık gösterip göstermediğini belirlemek için çok faktörlü varyans analizi (MANOVA),
- Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalıkları cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyona göre farklılık gösterip göstermediğini belirlemek için çok faktörlü varyans analizinden (MANOVA),
- Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalıkları siber saldırı-tehdit kavramını duyup duymama ve bu konuda eğitim alıp almama durumuna göre farklılık gösterip göstermediğini belirlemek için çok faktörlü varyans analizinden (MANOVA) yararlanılmıştır.

Ölçümler sonunda elde edilen verilerin analizinde 0,05 anlamlılık düzeyi esas alınmış ve analiz sonucu elde edilen bulgular 0,95 güven aralığında değerlendirilmiştir.

6. Bulgular ve Yorum

6.1. Çağrı merkezi çalışanlarının demografik özelliklerine ilişkin bulgular

Araştırmanın "Çağrı merkezi çalışanlarının cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyonuna ilişkin dağılımı nedir?" sorusuna ilişkin bulgular Tablo 1'de verilmiştir.

Tablo 1: Çağrı Merkezi Çalışanlarının Cinsiyet, Yaş, Çalışılan Yıl ve Çağrı Merkezindeki Pozisyonuna İlişkin Dağılımı

Demografik Özellikler			**f**	**%**
Cinsiyet	1	Kadın	28	58,3
	2	Erkek	20	41,7
		Toplam	**48**	**100**
Yaş	2	16-20	3	6,2
	3	21-25	13	27,1
	4	25-30	17	35,4
	5	31 ve üstü	15	31,2
		Toplam	**48**	**100**
Çalışılan Yıl	1	1-5 yıl	34	70,8
	2	6-10 yıl	7	14,6
	3	11-15 yıl	2	4,2
	4	16-20 yıl	5	10,4
		Toplam	**48**	**100**
Pozisyon	1	Çağrı alıcı	32	66,7
	2	Çağrı yönlendirici	8	16,7
	3	Diğer	8	16,7
		Toplam	**48**	**100**

Araştırmaya katılanların %58,3'ü kadın, %41,7'si erkektir. Yaş aralıklarına bakıldığında %35,4'ünün 25-30 yaş aralığında olduğu görülmektedir. Bu meslekte çalıştıkları yıl sorulduğunda ise %70,8'i 1-5 yıl aralığında bu mesleği yaptıklarını belirtmişlerdir. Çağrı merkezi çalışanlarının yaş grubu ve mesleki deneyimleri birbirine orantılı olup meslekte çok uzun yıllar çalışmadıklarını söyleyebiliriz. Mesleğin stresli ve yoğun olması bu mesleğin kısa sürede terk edilmesine neden olmaktadır. Araştırmaya katılanların %66,7'sinin çağrı alıcı pozisyonunda çalıştığı görülmektedir. Çağrı alıcı pozisyonu, çağrı merkezi teknolojilerini birebir kullanılan bir pozisyon olarak ifade edilebilir.

6.2. Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalık düzeyleri

Araştırmanın, "Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalık düzeyleri nedir?" sorusuna ilişkin bulgular Tablo 2'de verilmiştir.

Tablo 2: Çağrı Merkezi Çalışanlarının Çağrı Merkezi Teknolojileri Farkındalık Düzeylerine İlişkin İstatistikler

Çağrı merkezi teknolojileri	**N**	$\bar{x}$	**S**
Kulaklık ve mikrofon (çağrı dinleme ve yanıt sistemleri)	48	**3,90**	0,951
İnternet bağlantısı (kablolu veya kablosuz)	48	**3,85**	1,052
Bilgisayar donanımı (ekran, klavye, fare, yazıcı vb.)	48	3,83	1,173
Çağrı merkezi santral yazılımı (çağrı kayıtları)	48	3,19	1,315
İş Takibi-Harita-Telsiz yazılımları ve teknolojileri	48	3,02	1,329

Softphone çevirici yazılımları (bilgisayar üzerinde arama yapmaya yardımcı yazılımlar)	48	2,65	1,280
Güvenlik Duvarı (Firewall)	48	**2,31**	1,133
Telsiz,uydu telefonu,harita vb iletişim araçları-yazılımları	48	**2,29**	1,383
Genel Ortalama:		**3,13**	

(**N**: Çalışma grubu katılımcı sayısı, x̄: Aritmetik ortalama, **S**: Standart sapma)

Araştırmaya katılanların çağrı merkezi teknolojileri ile farkındalık düzeylerine ilişkin ortalamalara bakıldığında (Tablo 2); kulaklık ve mikrofon (x̄=3,90) ile internet bağlantısı (x̄=3,85) farkındalık düzeylerinin diğer çağrı merkezi teknolojileri farkındalık düzeylerine göre daha fazla olduğu görülmektedir. Araştırmaya katılanların %66,7 oranında çağrı alıcı pozisyonunda çalıştığı düşünülecek olursa teknik konulardan çok çağrı merkezi teknolojileri ile ilgili sadece kendi kullandıkları teknolojileri bilmeleri anlamlı bir sonuç olarak değerlendirilebilir. Telsiz, uydu telefonu, harita vb.iletişim araçları yazılımı (x̄=2,29) konusunda farkındalığın düşük çıkması da bu yönde değerlendirilebilir. Ayrıca bilgisayarlarda özellikle siber saldırılara karşı bilgisayar ve sunucular arasında gezen verilerin güvenilirliğini denetleyen firewall yani güvenlik duvarı farkındalıklarının (x̄=2,31) düşük düzeyde olması yine yazılımlar ve siber saldırılara karşı önlem alma konusunda yetersiz olunduğunun göstergesi olarak ortaya çıkmaktadır. Sadece çağrı alma ve çağrı yönlendirme pozisyonlarında oldukları düşünülürse araştırmaya katılanların pozisyonları dolayısıyla bu tür yazılımsal ve teknik konulara vakıf olmamaları doğal bir sonuç olarak değerlendirilebilir.

6.3. Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalık düzeyleri

Araştırmanın, "Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalık düzeyleri nedir?" sorusuna ilişkin bulgular Tablo 3'de verilmiştir.

Tablo 3: Çağrı Merkezi Çalışanlarının Siber Saldırı-Tehdit Teknolojileri Farkındalık Düzeylerine İlişkin İstatistikler

Siber Saldırı-Tehdit Teknolojileri	**N**	x̄	**S**
Taciz saldırıları (dolandırıcılık, tele-satış, tanıtım, korkutma, propaganda vb.)	48	**3,23**	1,418
Robot arama aldatmacılığı, ses kimlik avcılığı ve Spam	48	3,02	1,466
Finansal dolandırıcılık ve sosyal mühendislik saldırıları	48	2,92	1,514
Servis hırsızlığı ve telefon pompalama	48	2,52	1,557
Telefon DOS saldırıları (tDOS: telephony denial of service attack)	48	2,08	1,235
Modem / ISP aramaları ve faks istismarı	48	1,81	1,104
Sosyal tDOS saldırıları	48	1,67	1,018
SIP paket/ağ seviyesinde saldırılar	48	1,67	1,038
Genel Ortalama:		**2,36**	

(**N**: Çalışma grubu katılımcı sayısı, x̄: Aritmetik ortalama, **S**: Standart sapma)

Tablo 3'deki verilere göre, çağrı merkezi çalışanlarının taciz saldırıları farkındalık düzeyleri (x̄=3,23) ile robot arama aldatmacılığı farkındalık düzeylerinin (x̄=3,02) diğerlerine göre yüksek olduğu görülmektedir. Özellikle çağrı merkezlerinde telefonla iletişim alanındaki siber-tehdit farkındalıklarının oranının yüksek olduğu bulgulanmıştır. Çalışmaya katılanların çoğunun çağrı alıcı pozisyonunda olduğu düşünülecek olursa özellikle taciz ve dolandırıcılık farkındalığının yüksek olması doğru orantılı bir sonuç olarak yorumlanabilir. Ayrıca, katılımcıların sosyal tDOS (x̄=1,67) ve SIP paket/ağ seviyesindeki saldırılar (x̄=1,67) konusunda farkındalık düzeylerinin düşük

olduğu bulgulanmıştır. Bu bulgu, çağrı merkezi çalışanlarının daha teknik olan bu konularda bilgi düzeylerinin artırılması gerektiğini de göstermektedir.

6.4. Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalıklarının cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyona göre farklılıkları

Araştırmanın, "Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalıkları cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyona göre farklılık göstermekte midir?" sorusuna ilişkin bulgular Tablo 4'de verilmiştir.

Tablo 4: Çağrı Merkezi Çalışanlarının Çağrı Merkezi Teknolojileri Farkındalıklarının Cinsiyet, Yaş, Çalışılan Yıl ve Çağrı Merkezindeki Pozisyona Göre Farklılıklarına İlişkin Çok Faktörlü Varyans Analizi (MANOVA) Sonuçları

Bağımlı Değişken:Çağrı Merkezi Teknolojileri Farkındalıkları

Varyansın Kaynağı	KT	SD	KO	F	p
Cinsiyet	2,502	1	2,502	3,009	0,097*
Yaş	0,891	3	0,297	0,357	0,785*
Calışılan Yıl	2,134	2	1,067	1,283	0,298*
Pozisyon	0,889	2	0,444	0,534	0,594*
Hata	17,463	21	0,832		
Toplam	504,125	48			
Düzeltilmiş Toplam	33,811	47			

* p>0.05 (KT: Kareler Toplamı, SD: Serbestlik Derecesi, KO: Kareler ortalaması)

Tablo 4'teki çok faktörlü varyans analizi sonuçları incelendiğinde, çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalık düzeylerinin cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyonu değişkenlerine göre anlamlı bir farklılık göstermediği görülmektedir (p>0.05). Bu bulguya göre, çağrı merkezi çalışanlarının cinsiyetinin, yaşının, çalıştığı yılın ve çağrı merkezindeki pozisyonunun çağrı merkezi teknolojilerine ilişkin farkındalıklarında önemli bir etken olmadığı söylenebilir.

6.5. Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalıklarının çağrı merkezi sistemleri güvenliğini duyup duymama ve bu konuda eğitim alıp almama durumuna göre farklılıkları

Araştırmanın, "Çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalıkları çağrı merkezi sistemleri güvenliğini duyup duymama ve bu konuda eğitim alıp almama durumuna göre farklılık göstermekte midir?" sorusuna ilişkin bulgular Tablo 5 ve Tablo 6'da verilmiştir.

Tablo 5: Çağrı Merkezi Çalışanlarının Çağrı Merkezi Sistemleri Güvenliğini Duyup Duymama ve Bu Konuda Eğitim Alıp Almama Durumuna İlişkin İstatistikler

Çağrı merkezleri sistemleri güvenliği	E/H	f	%
Çağrı merkezi sistemleri güvenliğini duyup duymama (CMSGduy)	Evet	32	66,7
	Hayır	16	33,3
Çağrı merkezi sistemleri güvenliği konusunda eğitim alıp almama (CMSGegt)	Evet	9	18,8
	Hayır	39	81,2

Çağrı merkezi çalışanlarına çağrı merkezi güvenliğini duyup duymadıkları sorulduğunda, katılımcıların çoğunun (n=32; %66,7) böyle bir kavramı duydukları belirlenmiştir. Hemen bu sorunun arkasından duymalarına karşın bu konuda eğitim alıp almadıkları sorulduğunda ise katılımcıların çoğunun (n=39; %81,2) hayır cevabı

verdiği Tablo 5'te görülmektedir. Güvenlik sorununun farkında olunmasına karşın buna karşı bir önlem alınmaması düşündürücüdür. Aynı zamanda çağrı merkezi çalışanlarının işgören devir hızının çok yoğun bir sektör olduğu gerçeğinden yola çıkarak insan kaynağının eğitimine fazla yatırım yapmadıkları gibi bir sonuçta buradan çıkmaktadır.

Tablo 6: Çağrı Merkezi Çalışanlarının Çağrı Merkezi Teknolojileri Farkındalıklarının Çağrı Merkezi Sistemleri Güvenliğini Duyup Duymama ve Bu Konuda Eğitim Alıp Almama Durumuna Göre Farklılıklarına İlişkin Çok Faktörlü Varyans Analizi Sonuçları

Bağımlı Değişken: Çağrı Merkezi Teknolojileri Farkındalıkları

Varyansın Kaynağı	KT	SD	KO	F	p
CMSGduy	0,053	1	0,053	0,077	0,783*
CMSGegt	2,293	1	2,293	3,341	0,074*
Hata	30,892	45	0,686		
Toplam	504,125	48			
Düzeltilmiş Toplam	33,811	47			

* p>0.05 (KT: Kareler Toplamı, SD: Serbestlik Derecesi, KO: Kareler ortalaması)

Tablo 6'daki çok faktörlü varyans analizi sonuçları incelendiğinde ise, çağrı merkezi çalışanlarının çağrı merkezi teknolojilerine ilişkin farkındalık düzeylerinin çağrı merkezi sistemleri güvenliğini duyup duymama ve bu konuda eğitim alıp almama durumuna göre anlamlı bir farklılık göstermedikleri görülmüştür (p>0,05). Bu bulguya göre, çağrı merkezi çalışanlarının çağrı merkezine ilişkin farkındalık düzeylerinde çağrı merkezi sistemleri güvenliğini duyup duymama ve bu konuda eğitim alıp almama durumunun önemli bir farklılık oluşturmadığı söylenebilir.

6.6. Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalıklarının cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyona göre farklılıkları

Araştırmanın, "Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalıkları cinsiyet, yaş, çalışılan yıl ve çağrı merkezindeki pozisyona göre farklılık göstermekte midir?" sorusuna ilişkin bulgular Tablo 7'de verilmiştir.

Tablo 7: Çağrı Merkezi Çalışanlarının Siber Saldırı-Tehdit Teknolojileri Farkındalıklarının Cinsiyet, Yaş, Çalışılan Yıl ve Çağrı Merkezindeki Pozisyona Göre Farklılıklarına İlişkin Çok Faktörlü Varyans Analizi (MANOVA) Sonuçları

Bağımlı Değişken: Siber Saldırı Tehdit Teknolojileri Farkındalığı

Varyansın Kaynağı	KT	SD	KO	F	p
Cinsiyet	1,729	1	1,729	1,928	0,180*
Yaş	0,453	3	0,151	0,168	0,916*
Çalışılan Yıl	10,364	2	5,182	5,778	0,010
Pozisyon	0,772	2	0,386	0,431	0,656*
Hata	18,833	21	0,897		
Toplam	315,688	48			
Düzeltilmiş Toplam	47,307	47			

* p>0.05 (KT: Kareler Toplamı, SD: Serbestlik Derecesi, KO: Kareler ortalaması)

Tablo 7'deki çok faktörlü varyans analizi sonuçlarına incelendiğinde çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalıklarının cinsiyet, yaş ve çağrı merkezindeki pozisyona göre anlamlı bir farklılık

göstermediği (p>0.05), buna karşın çalışılan yıla göre (p<0.010) anlamlı bir farklılık gösterdiği görülmektedir. Bu bulguya göre, çağrı merkezinde çalışanların çalıştıkları yıllar açısından siber saldırı-tehdit konusunda önemli bir farklılık ortaya çıktığı söylenebilir. Diğer bir ifadeyle, çağrı merkezi çalışanları zaman içerisinde yaptıkları iş açısından deneyim kazanmakta ve özellikle siber saldırı-tehdit konusunda bilgi sahibi olmakta ve farkında olmaktadırlar.

6.7. Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalıkları siber saldırı-tehdit kavramını duyup duymama ve bu konuda eğitim alıp almama durumuna göre farklılıkları

Araştırmanın, "Çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojileri farkındalıkları siber saldırı-tehdit kavramını duyup duymama ve bu konuda eğitim alıp almama durumuna göre farklılık göstermekte midir?" sorusuna ilişkin bulgular Tablo 8 ve Tablo 9'da verilmiştir.

Tablo 8: Çağrı Merkezi Çalışanlarının Siber Saldırı-Tehdit Kavramını Duyup Duymama ve Bu Konuda Eğitim Alıp Almama Durumuna İlişkin İstatistikler

Siber saldırı-tehdit	E/H	f	%
Siber saldırı-tehdit kavramını duyup duymama (SiberSduy)	Evet	40	83,3
	Hayır	8	16,7
Siber saldırı-tehdit konusunda eğitim alıp almama (SiberSegt)	Evet	8	16,7
	Hayır	40	83,3

Çağrı merkezi çalışanlarına siber saldırı-tehdit kavramını duyup duymadıkları sorulduğunda, katılımcıların çoğunun (n=40; %83,3) böyle bir kavramı duydukları belirlenmiştir. Bu sorunun arkasından duymalarına karşın bu konuda eğitim alıp almadıkları sorulduğunda ise katılımcıların çoğunun (n=40; %83,3) hayır cevabı verdiği Tablo 8'te görülmektedir. Çağrı merkezi çalışanlarından siber saldırı-tehdit kavramını duymalarına karşın bu konuda daha önce eğitim almayanların çoğunlukta olması önemli bir sorunu ortaya çıkarmaktadır. Dolayısıyla, çağrı merkezi çalışanlarına siber saldırı-tehdit konusunda bir eğitim verilmesi ya da çalışanların bu konuda bir eğitim alarak bu soruna çözüm üretilmesi gerekliliği ortadadır.

Tablo 9: Çağrı Merkezi Çalışanlarının Siber Saldırı-Tehdit Teknolojileri Farkındalıkları Siber Saldırı-Tehdit Kavramını Duyup Duymama ve Bu Konuda Eğitim Alıp Almama Durumuna Göre Farklılıklarına İlişkin Çok Faktörlü Varyans Analizi (MANOVA) Sonuçları

Bağımlı Değişken: Siber Saldırı-Tehdit Teknolojileri Farkındalıkları

Varyansın Kaynağı	KT	SD	KO	F	p
SiberSduy	0,609	1	0,609	0,640	0,428*
SiberSegt	4,348	1	4,348	4,569	0,038
Hata	42,822	45	0,952		
Toplam	315,688	48			
Düzeltilmiş Toplam	47,307	47			

* p>0.05 (KT: Kareler Toplamı, SD: Serbestlik Derecesi, KO: Kareler ortalaması)

Tablo 9'daki çok faktörlü varyans analizi sonuçları incelendiğinde ise, çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojilerine ilişkin farkındalık düzeylerinin siber saldırı-tehdit kavramını duyup duymama durumuna göre anlamlı bir farklılık göstermediği (p>0,05), buna karşın siber saldırı-tehdit teknolojileri konusunda eğitim alıp almama durumuna göre anlamlı bir farklılık gösterdiği görülmektedir (p<0,05). Bu bulguya göre, çağrı merkezi çalışanlarının çağrı merkezine ilişkin farkındalık düzeylerinde siber saldırı-tehdit teknolojileri kavramını duyup duymamasının önemli bir farklılık oluşturmadığı, buna karşın bu konuda eğitim alıp almama durumunun önemli bir faktör olduğu söylenebilir.

SONUÇ

Temel amacı, çağrı merkezi çalışanlarının çağrı merkezi teknolojileri ve siber saldırı-tehdit farkındalıklarını ortaya koymak olan ve nicel verilere dayalı tarama araştırması olarak gerçekleştirilen araştırmada, çağrı merkezi çalışanlarının çağrı merkezi teknolojileri ve siber saldırı-tehdit farkındalık düzeylerine ilişkin istatistiksel çözümlemeleri içeren araştırma bulguları ortaya konulmuştur.

Araştırmaya katılanların %58,3'ü kadın, %41,7'si erkektir. Araştırmaya katılanların yaş aralıklarına bakıldığında %35,4'ünün 25-30 yaş aralığında olduğu ve %70,8'inin bu mesleği 1-5 yıl aralığında yaptığı görülmektedir. Dolayısıyla çağrı merkezi çalışanlarının dinamik bir meslek grubu olduğu açıktır. Araştırmaya katılanların çağrı alıcı ve çağrı yönlendirici pozisyonunda çalışanlardan oluşması ve mesleğin stresli ve yoğun olması bu mesleğin kısa sürede terk edilmesi gibi bir sonucu çıkarmaktadır.

Çağrı alıcı ve yönlendirici pozisyonunda çalışanların daha çok çağrı merkezi teknolojilerinden bilgisayar, kulaklık, mikrofon, internet bağlantısı gibi konularda farkındalıklarının daha fazla olduğu görülmektedir. Araştırmaya katılanların %66,7 oranında çağrı alıcı pozisyonunda çalıştığı düşünülecek olursa teknik konulardan çok çağrı merkezi teknolojileri ile ilgili sadece kendi kullandıkları teknolojileri bilmeleri anlamlı bir sonuç olarak değerlendirilmektedir. Telsiz, uydu telefonu, harita vb.iletişim araçları yazılımı konusunda farkındalığın düşük çıkması da bu yönde değerlendirilebilir. Bilgisayarlarda özellikle siber saldırılara karşı bilgisayar ve sunucular arasında gezen verilerin güvenilirliğini denetleyen firewall yani güvenlik duvarı konusunda farkındalıklarının da zayıf olması yine yazılımlar ve siber saldırılara karşı önlem alma konusunda yetersiz olunduğunun göstergesi olarak karşımıza çıkmaktadır. Pozisyonları dolayısıyla çalışma grubunun sadece çağrı alma ve çağrı yönlendirme pozisyonlarında oldukları düşünülürse bu tür yazılımsal ve teknik konulara vakıf olmamaları doğal bir sonuç olarak değerlendirilebilir.

Araştırma bulguları ışığında, çağrı merkezi çalışanlarının çağrı merkezi teknolojileri farkındalıklarının orta düzeyde, siber-saldırı tehdit teknolojileri farkındalıklarının ise düşük düzeyde olduğu ve bu teknolojilere ilişkin farkındalıklarının demografik değişkenlere göre önemli bir farklılık göstermediği sonucuna varılmıştır. Buna ilaveten araştırmada, çağrı merkezi çalışanlarının siber saldırı-tehdit teknolojilerine ilişkin farkındalık düzeylerinin çalışılan yıl ve eğitim alıp almama durumlarına göre önemli bir farklılık gösterdiği de görülmüştür.

Bu araştırma ile çalışanların sosyal ve SIP paket/ağ seviyesindeki saldırılar konusunda farkındalık düzeylerinin düşük olduğu bulgulanmıştır. Sonuçlar daha teknik olan bu konularda çağrı merkezi çalışanlarının bilgi düzeylerinin artırılması gerektiğini de göstermektedir. Ayrıca, çalışanlara siber saldırı-tehditlerine karşı da farkındalık kazandırılmalı ve bu tür olaylarla karşılaştıklarında önlem alabilmeleri ve ilgili çözüm yolları üretebilmeleri için yol gösterici olunmalıdır. Bunun sağlanması için çağrı merkezi çalışanlarına siber saldırı-tehdit konusunda bir eğitim verilmesi ya da çalışanların bu konuda bir eğitim almaya teşvik edilmeleri önerilebilir. Böylelikle bu soruna çözüm üretmeleri mümkün olabilir.

Araştırma, Antalya bölgesinde hizmet veren çağrı merkezlerinde çağrı alıcı ve çağrı yönlendirici gibi benzer konumlarda çalışanlardan elde edilen veriler ve bu verilere ilişkin elde edilen istatistiksel analizler sonucu elde edilen bulgular ile sınırlı olduğundan bu araştırmaya ilgi duyan alanyazındaki araştırmacılara da fazla katılımcının bulunduğu farklı bölgelerdeki çağrı merkezlerinde ve farklı değişkenler boyutunda araştırmalar yapmaları önerilebilir.

KAYNAKÇA

AKSIN, Z., ARMONY, M. ve MEHROTRA, V. (2009). **The Modern Call Center: A Multi-Disciplinary Perspective on Operations** Management Research, Production and Operations Management, 16 (6), 665-688.

AÇIKGÖZ, O. (2016). **Kişisel Verilerin Hukuka Aykırı Şekilde Elde Edilmesi ve İnternet Bankacılığında Kullanılması Sonucu Malvarlığı Zarara Uğratılan Bankaya Karşı Mevduat Sahibinin Hukuki Sorumluluğu.** Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi , 22 (1), 389-432.

BAPTISTA, J., NEWELL, S. ve CURRIE, W. (2010). **Paradoxial Effects of Institutionalisation on the Strategic Awaraness of Technology in Organizations,** The Journal of Strategic Information Systems, 19 (3), 171-183.

BERNETT, H. ve JARAMİLLO, M.L. (2001). **Assesing Web-enabled Call Center Technologies,** IT Professional, 3 (3), 24-30.

BOYD, C. (2002). **Customer Violence and Employee Health and Safety,** Work, Employment & Society, 16 (1), 151-169.

BROWN, L., GANS, N, MANDELBAUM, A., SAKOV, A. SHEN, H., ZELYTN, S., ZHAO, L. (2005). **Statistical Analysis of a Telephone Call Center,** Journal of the American Statistical Association , 100 (469), 36-50.

COHEN, F. (1999). **Simulating Cyber Attacks, Defences and Consequences,** Computers & Security, 18 (6), 479-518.

DEAN, A.M. (2004). **Rethinking customer expectations of service quality: are call centers different?,** Journal of Service Marketing, 18 (1), 60-78.

DUTT, V., AHN, Y ve GONZALEZ, C. (2013). **Cyber Situation Awarenness: Modelling Detection of Cyber Attacks with Instance-Based Learning Theory,** The Journal of the Human Factors and Ergonomics Society, 55 (3), 605-618.

GANS, N., KOOLE, G. ve MANDELBAUM, A. (2003). **Telephone Call Centers: Tutorial, Review, and Research Prospects,** Manufacturing & Service Operations Management, 5 (2), 79-141.

HOLMAND, D., CHİSSİCK, C. ve TOTTERDELL, P. (2002). **The Effects of Performance Monitoring on Emotional Labor and Well-Being in Call Centers,** Motivation and Emotion, 26 (1), 57-81.

KOCABAŞ, İ. (2017). **Çağrı Merkezi Müşteri Temsilcisinin İmajının Müşteri Memnuniyeti Üzerindeki Rolü.** Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi , 5 (1), 118-147.

LALA, C. ve PANDA, B. (2001). **Evaluating Damage from Cyber Attacks: A Model and Analysis,** IEEE Transactions on Systems, Man, and Cybernetics, 31 (4), 300-310.

ROBINSON, G., ve MORLEY, C. (2006). **Call Centre Management: Responsibilities And Performance.** International Journal of Service Industry Management , 17 (3), 284-300.

SARIYER, N. (2007). **Çağrı Merkezi Tüketici Profili: Banka Çağrı Merkezlerinde Bir Uygulama.** Erzurum: Atatürk Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi.

SEÇKİN, E., ve ÖKTEN, A. N. (2009). **Az Gelişmiş Bölgelerin Gelişmesinde Bir Fırsat Olarak Çağrı Merkezleri.** MEGARON , 191-202.

TAŞKIN, D., ve TAŞKIN, Ç. (2018)**. Çağrı Merkezi Hizmetlerinde Müşteri Beklentisi Boyutlarının Müşteri Tatmini Üzerindeki Etkisinin PLS-Sem İle Ölçümü .** Journal Of Business Research Turk , 10 (1), 465-481.

VOICE & UNIFIED COMMUNICATIONS (2014). **Voice & Unified Communications State of Security Report 2014.** San Antonio: Secure Logix.

YAVUZ, U., ve LELOĞLU, H. (2011). **Müşteri İlişkileri Yönetiminde Çağrı Merkezlerinin Yeri:Çağrı Merkezi Örneği.** Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi , 11-24.