Bu proje Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.
This Project is co-funded by the European Union and the Council of Europe.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

TÜRKİYE'DE GÖREV YAPAN CUMHURİYET SAVCILARI VE KOLLUK KUVVETLERİ İÇİN **SİBER SUÇ SORUŞTURMALARI KILAVUZU**

"Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi İhlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması" Avrupa Birliği ve Avrupa Konseyi Ortak Projesi

Hazırlayanlar
A. Kemal KUMKUMOĞLU
Dr. Michael JAMEISON

TÜRKİYE'DE GÖREV YAPAN CUMHURİYET SAVCILARI VE KOLLUK KUVVETLERİ İÇİN

SİBER SUÇ SORUŞTURMALARI KILAVUZU

TÜRKİYE'DE GÖREV YAPAN CUMHURİYET SAVCILARI VE KOLLUK KUVVETLERİ İÇİN SİBER SUÇ SORUŞTURMALARI KILAVUZU

Hazırlayanlar
- A. Kemal KUMKUMOĞLU
- Dr. Michael JAMEISON

Bu Kılavuz "Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi İhlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması" Avrupa Birliği ve Avrupa Konseyi Ortak Projesi kapsamında hazırlanmıştır. Bu Proje Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmekte, Avrupa Konseyi tarafından yürütülmektedir. Projenin sözleşme makamı Merkezi Finans ve İhale Birimidir.

Tasarım
EPAMAT BASIM YAYIN PROMOSYON SAN.VE TİC.LTD.ŞTİ.
Ağaçişleri Sanayi Sitesi 1357. Sok. No: 41
Yenimahalle/ANKARA
Tel : (0312) 394 48 63 - 64
Faks : (0312) 394 48 65

Baskı
Tam Pozitif Reklam&Matbaa
Çamlıca Mahallesi Anadolu Bulvarı 145. Sokak 10/11
Yenimahalle/ANKARA
Tel: 0312 397 00 31 | Faks: 0312 397 86 12
E-Posta: pozitif@pozitifmatbaa.com

www.coe.int/tr/web/ankara
Avrupa Konseyi Ankara Program Ofisi
cas.ankara@coe.int
Ceza Adalet Sisteminin Güçlendirilmesi Projesi
cas_projesi
@project_cas
Ceza Adalet Sisteminin Güçlendirilmesi Projesi

Proje Paydaşları

- Türkiye Cumhuriyeti Anayasa Mahkemesi
- Yargıtay Başkanlığı
- Hakimler ve Savcılar Kurulu
- Türkiye Barolar Birliği
- Mali Suçları Araştırma Kurulu Başkanlığı (MASAK)
- Jandarma Genel Komutanlığı
- Emniyet Genel Müdürlüğü
  - Siber Suçlarla Mücadele Daire Başkanlığı
  - Terörle Mücadele Dairesi Başkanlığı
  - Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı
- Bilgi Teknolojileri ve İletişim Kurumu
- Adli Tıp Kurumu

İÇİNDEKİLER

1. Giriş

Giderek dijitalleşen bir dünyada, modern teknolojiler günlük hayatımızın bir parçası hâline gelmiştir. E-postalar, mobil haberleşme programları, çevrimiçi bankacılık, çevrimiçi alışveriş, medya akışı (streaming) hizmetleri, çevrimiçi oyunlar, akıllı evler/şehirler/arabalar, kripto para birimleri ve sosyal medya, internetin günlük hayatımız üzerindeki etkisinin sadece birkaç örneğidir.

İnsanların yeni teknolojileri kullandığı ve benimsediği hızda, suçlular da aynı teknolojileri kendi menfaatleri için kullanmaktadır. Başka yerlerde olduğu gibi Türkiye'de de siber suçlular, sadece masum vatandaşları çevrimiçi ortamda dolandırmak, taciz etmek, takip etmek, istismar etmek ve tehdit etmekle kalmamakta, aynı zamanda kara para aklamak ve çocuk istismarı materyalleri, silah ve uyuşturucu gibi yasadışı maddelerin kaçakçılığını yapmak için de interneti kötüye kullanmaktadır. Bu örnekler yeterince geniş kapsamlı değilmiş gibi, internet ve elektronik cihazlar ayrıca cinayet, suistimal ve terör eylemleri de dâhil, fiziksel dünyadaki geleneksel suçların planlaması, koordine edilmesi ve hatta kolaylaştırılması için kötüye kullanılmaktadır.

Adli makamların (polis memurları ve cumhuriyet savcıları) temel görevlerinden biri, suçları önleyerek, soruşturarak ve kovuşturarak vatandaşları korumaktır. Bu durum, yüzyıllar boyunca sadece fiziksel dünyada işlenen suçlar için geçerli olmuştur. Zamanın değişmesiyle birlikte, vatandaşları koruma görevinin dijital dünyada da yerine getirilmesi gerektiği aşikârdır. Bunun yapılabilmesi için, ceza adaleti makamlarının siber suçları ve siber ortamda gerçekleştirilen geleneksel suçları önleme, soruşturma ve kovuşturma yetkinliklerini geliştirmeleri gerekmektedir.

Bu kılavuzda, siber suçların soruşturulması ve elektronik veya dijital delillerin işlenmesindeki en iyi uygulamalar sunulacaktır.[1] Kılavuzda, elektronik

1 Bu belgede "Elektronik" ve "dijital" delil terimleri eşanlamlı olarak kullanılmıştır.

delillerle ilgili olarak, Türkiye'deki Cumhuriyet Savcıları ve Kolluk Kuvvetlerinin kullanımına açık olan aşağıdaki Avrupa Konseyi araçlarına atıfta bulunulacaktır:

1. "Elektronik Delil Kılavuzu"
2. "Adli Bilişim Laboratuvarı Yönetimi ve Prosedürlerine Yönelik Temel Kılavuz"
3. "Elektronik delillerin toplanması, analizi ve sunumuna yönelik Standart Çalışma Prosedürleri"
4. "Kripto Para Birimlerine Elkoyulmasına İlişkin Kılavuz"
5. "Kolluk Kuvvetleri için Siber Suçlar ve Elektronik Deliller Konusunda Eğitim Stratejileri Geliştirme Kılavuzu"

Bu araçlara Avrupa Konseyi "Octopus Platformu" üzerinden erişilebilir.[2]

2 Avrupa Konseyi "Octopus Platformu" – Materyaller bölümü: https://www.coe.int/en/web/octopus/training

2. Kılavuzun amacı

Bu kılavuzun amacı, siber suç soruşturmalarında siber suç soruşturmacısı veya uzmanlaşmış siber suç birimlerinin bir parçası olmayan uygulayıcılara, siber suç mağdurlarının şikâyetlerini alabilmeleri ve soruşturmanın ilk evresini yürütebilmeleri için destek ve ön rehberlik sağlamaktır.

Bu kılavuz, Türkiye'deki uygulayıcılar tarafından dile getirilen bir ihtiyaca yanıt olarak geliştirilmiştir ve bir dizi amaca hizmet etmektedir:

1. Kılavuz, Türkiye'deki siber suç soruşturmalarında uygulayıcılara yönelik prosedürlerin geliştirilmesi için bir başlangıç noktası teşkil edebilir.
2. Kılavuz ayrıca, siber suç soruşturmalarıyla ilgilenen yetkililer tarafından da doğrudan uygulanabilir. Bununla birlikte, yetkililerin bu tür bir uygulamanın Türkiye'deki güncel hukuki sisteme uygunluğunu sağlamaları gerekecektir.
3. Bu kılavuzda açıklanan prosedürler, siber suç soruşturmalarına ilk müdahale eden kişilerin izleyeceği teknik ve taktik prosedürlerin daha iyi anlaşılmasını sağlamak amacıyla, polis memurları veya cumhuriyet savcılarına yönelik eğitim faaliyetlerinde kullanılabilir.
4. Kılavuz, siber suç soruşturmalarında uygulayıcıların yürüteceği işlemlerin kritik olması nedeniyle, uygulayıcıların önemini özellikle vurgulamaktadır. Uygulayıcıların verileri zamanında toplayamaması hâlinde bu veriler yok olabilmektedir. Uygulayıcıların bir siber suç soruşturması karşısında yetkinlik gösterememesi, bu tür suçları ele alma kâbiliyetleriyle ilgili kolluk kuvvetlerine ve yargıya duyulan güveni ve bu makamların görünür itibarını doğrudan etkileyecektir.
5. Uygulamaya yönelik kılavuzun sadece Türkiye'deki en güncel yasal çerçeveye uygun olması değil, aynı zamanda âdil yargılanma hakkı

(Madde 6), özel hayata ve aile hayatına saygı hakkı (Madde 8) ve ifade özgürlüğüne (Madde 10) özellikle dikkat ederek, Avrupa İnsan Hakları Sözleşmesi'nde (AİHS) belirtilen temel hakların ihlâlini önleyebilecek doğru bilgiler vermesi de amaçlanmaktadır.[3]

–

Bu kılavuzun adım adım talimatlar içeren bir kullanım kılavuzu olması amaçlanmadığı gibi, kılavuz Standart Çalışma Prosedürleri (SOP) olarak da kullanılmamalıdır. Bunun yerine kılavuz, siber suçların özelliklerine odaklanmakta ve siber suç soruşturmalarının ilk aşamalarında atılması gereken adımların ana hatlarını sunmaktadır. Kılavuz, daha derinlemesine bir anlayış sunmak amacıyla, karmaşık soruşturmaları destekleyebilecek bazı faydalı kaynaklar sağlamakta; ayrıca en sık görülen siber suç olaylarına genel bir bakış da sunmaktadır.

3 Buna paralel olarak, S. ve Marper-Birleşik Krallık davasında (Büyük Daire, 4 Aralık 2008, 30562/04 ve 30566/04) AİHM: *"Çağdaş bilimsel tekniklerin ceza adaleti sisteminde kullanılmasına, bu tekniklerin geniş bir şekilde kullanılmasından doğan avantajlar ile özel hayatın korunmasıyla ilgili temel menfaatler arasında dikkatli bir denge kurulmadan, ne pahasına olursa olsun, izin verilmiş olsaydı, Sözleşme'nin 8. Maddesi'nin sağladığı koruma kabul edilemez bir şekilde zayıflardı. Yeni teknolojilerin gelişiminde öncü rol oynama iddiasında olan her ülke, bu alanda âdil bir denge bulmaya yönelik özel sorumluluk taşımaktadır."* demiştir.

3. Siber suçlar ve siber ortamda gerçekleştirilen geleneksel suçlar

3.1. Siber suçlar

Siber suçun ne olduğuna dair uluslararası düzeyde mutabık kalınmış bir açıklama veya tanım bulunmamaktadır. Bazı yargı sistemleri, siber suçları bir bilgisayar veya dijital cihaz aracılığıyla gerçekleştirilen herhangi bir suç olarak tanımlarken, bazı sistemler ise daha spesifik olarak, bilgisayar aracılığıyla, bir mağdur veya benzeri bir kişi tarafından kullanılan bir bilgisayara veya başka bir cihaza karşı siber saldırı gerçekleştirilmesi olarak tanımlamaktadır.

Bu belgenin amacı doğrultusunda, siber suçlar, Budapeşte Siber Suç Sözleşmesi'nin 2 ilâ 9. maddeleri arasında tanımlanan suçlardır ve aşağıdakileri içermektedir.[4]

- Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar;
  - Yasadışı Erişim – Madde 2
  - Yasadışı Müdahale – Madde 3
  - Verilere Müdahale – Madde 4
  - Sistemlere Müdahale – Madde 5
  - Cihazların Kötüye Kullanımı – Madde 6
  - Bilgisayarla ilişkili Sahtecilik– Madde 7
  - Bilgisayarla ilişkili Dolandırıcılık – Madde 8
- İçerikle İlişkili Suçlar
  - Çocuk Pornografisiyle İlişkili Suçlar – Madde 9

Türkiye'de görülen belirli siber suç türleri, Bölüm 5'te ayrıntılı olarak açıklanmıştır.

4 https://rm.coe.int/1680081561

3.2. Siber ortamda gerçekleştirilen geleneksel suçlar

Bu belge kapsamında bu tür suçlar, çevrimiçi olarak veya bir bilgisayar (veya başka bir dijital cihaz) kullanılarak gerçekleştirilen ancak bu tür bir teknoloji kullanılmadan da işlenebilecek diğer tüm suçlar olarak kabul edilmektedir. Bu suç türüne örnek olarak çevrimiçi zorbalık ve sosyal mühendislik saldırıları verilebilir.

4. Elektronik delillerin tanımı

Siber suç soruşturmalarından bahsederken kullanılan elektronik delillerin birçok tanımı bulunmaktadır. Bu kılavuz kapsamında, Avrupa Konseyi Elektronik Delil Kılavuzu'nda yer alan tanım esas alınmıştır. Daha ayrıntılı bilgi için kılavuzun kendisini inceleyebilirsiniz[5].

Elektronik deliller, bilgisayarlar ve bunların çevresel aygıtları gibi elektronik cihazlardan, bilgisayar ağlarından, cep telefonlarından, dijital kameralar ve diğer mobil cihazlardan (veri depolama aygıtları dâhil) ve internetten elde edilmektedir. Elektronik delillerin içerdiği bilgi, bağımsız bir fiziksel forma sahip değildir.

Kendine has özellikleri göz önüne alındığında, elektronik delil, daha sonra yargılama sürecinde davaya konu vakayı kanıtlamak veya çürütmek için ihtiyaç duyulabilecek, dijital formatta üretilen, saklanan veya iletilen her tür bilgi olarak tanımlanabilir.

- Elektronik delillerin özellikleri
- Tecrübesiz kişiler tarafından görülemez
- Son derece uçucudur
- Olağan kullanımla değiştirilebilir veya imhâ edilebilir
- Bozulmadan çoğaltılabilir

Suçlular avlarının peşindeki avcılar gibidir ve dijital medyanın kitlesel kullanımı ve internet, suçlulara suç işlemeleri için yeni fırsatlar sağlamıştır. Suçlular, bu yeni iletişim kanallarını kötüye kullanarak geleneksel suçlar için yeni stratejiler geliştirmiş ve yeni suç kategorileri ortaya çıkmıştır. Sonuç olarak, hukuk sisteminin parçası olan herkesin farklı elektronik delil biçimlerine aşina olması ve bunlarla nasıl başa çıkılacağını bilmesi gerekmektedir.

5 "Elektronik Delil Kılavuzu - POLİS MEMURLARI, SAVCILAR VE HÂKİMLER İÇİN TEMEL BİR REHBER", Sürüm 2.1, 03/2020, Avrupa Konseyi, https://www.coe.int/en/web/octopus/training

Elektronik delilleri yargılama sürecine sunan tarafın, bu delillerin suçun işlendiği esnada mevcut bulunan aynı koşulları ve olgusal bilgileri yansıttığını gösterebilmesi gerekmektedir ve bu açıdan bakıldığında elektronik delillerin geleneksel delillerden bir farkı yoktur. Başka bir deyişle, bahse konu taraf, herhangi bir değişiklik, silme, ekleme veya başka türlü bir tahrifatın gerçekleşmediğini (veya gerçekleşmiş olamayacağını) ortaya koymakla yükümlüdür. Elektronik formatta saklanan her türlü veri veya bilgi, doğası gereği somut olmayan bir yapıya sahip olduğundan, bu tür veri ve bilgilerin manipüle edilmesi geleneksel delil türlerine kıyasla çok daha kolaydır ve bu durum bu veri ve bilgileri değiştirilmeye daha yatkın hâle getirmektedir. Söz konusu durum adalet sistemi için özel zorluklar yaratmıştır ve bu tür verilerin, sundukları kanıtların bütünlüğünü sağlamak için özel bir şekilde ele alınmasını gerektirmektedir.

Bu sebeple, elektronik delillerin korunması, tüm dünyada kabul görmüş beş ilkeye uygun biçimde ele alınmalıdır.

1. "Veri Bütünlüğü" - yapılan hiçbir işlem, daha sonra mahkemede dayanak olarak kullanılabilecek elektronik cihazları veya medyayı değiştirmemelidir.[6] Elektronik cihazlar ve veriler işlenirken, donanım ya da yazılım açısından herhangi bir değişiklik yapılmamalıdır. Dosyadan sorumlu kişi, olay yerinden toplanan materyalin bütünlüğünden ve dolayısıyla adli delil zincirinin oluşturulmasından sorumludur. Bazı durumlarda, potansiyel delillerin kaybolmasını önlemek amacıyla "canlı" bir bilgisayar sistemindeki verilere erişilmesi kararının verilmesi gerekebilir. Bu işlem, verileri asgari düzeyde etkileyecek şekilde ve bu konuda yetkin bir kişi tarafından gerçekleştirilmelidir.

2. "Denetim İzi" - elektronik deliller işlenirken yapılan tüm işlemlerin bir denetim izi veya başka bir kaydı oluşturulmalı ve söz konusu kayıtlar muhafaza edilmelidir. Bağımsız bir üçüncü taraf bu işlemleri incelediğinde aynı sonuca ulaşabilmelidir. Delillerin mahkemede hükme esas alınabilmesini sağlamak amacıyla, üçüncü bir tarafın, ilk müdahaleyi

6 Yargıtay, veri bütünlüğü ilkesini yinelerken, ilgili usûli güvencelere uyulmasının önemini vurgulamıştır: "Elkoyma işlemi sırasında sistemdeki bütün verilerin yedeklenmesi (imaj alma işlemi), yedeklenen kayıtların birer kopyasının istenmesi hâlinde şüpheliye veya vekiline verilmesi, bu hususun tutanağa geçirilerek imza altına alınması gerekmektedir. Yedekleme işlemi de mutlak suretle şüpheli ve/veya müdafisinin huzurunda yapılarak imaj alınmadan önce sisteme veri yerleştirildiği ve daha fazla sonra imaj alındığı şüphesi ortadan kaldırılmalıdır." (Yargıtay CGK., E. 2016/544 K. 2020/127 T. 25.2.2020)

yapan kişinin olay yerinde yaptığı işlemleri tekrar yapabilmesi ve bunun için de tüm işlemlerin doğru bir şekilde kaydedilmiş olması gerekmektedir. Elektronik delillere elkoyulması, bunlara erişilmesi, bu delillerin saklanması ve aktarılması ile ilgili tüm işlemler eksiksiz bir biçimde belgelenmeli, muhafaza edilmeli ve incelenmeye hazır olmalıdır.

3. "Uzman desteğinden" yararlanılmalıdır. Bir operasyon sırasında elektronik delillerin bulunabileceği düşünülüyorsa, dosyadan sorumlu kişi polisin adli bilişim birimini zamanında bilgilendirmelidir. Elektronik delillerin aranması ve bunlara elkoyulmasını gerektiren soruşturmalarda dışarıdan uzmanlara danışılması gerekebilir. Bu tarz uzmanların, gerekli bilgi, uzmanlık ve deneyime sahip olması ve aynı zamanda bu veya buna benzer ilgili belgelerde ortaya konulan ilkelere aşina olması gerekmektedir.

Anayasa Mahkemesi'ne göre, denetim izi ve uzman desteği alma ilkeleri, savunma hakları ve âdil yargılanma hakkıyla doğrudan ilişkilidir: "Dijital deliller üzerinde yapılacak teknik incelemenin suçların sübutu ve sanıkların bu suçlarla ilgisinin tespiti bakımından belirleyici olabileceği açıktır. Başvurucunun, dijital delillerin içindeki belgelerin kendisi tarafından oluşturulmadığı ve temin edilmemiş olduğu iddiası karşısında bu iddialarla ilgili olarak etkili bir şekilde savunma yapmaya imkân verecek bir erişimin sağlanmış olması ya da yargılama makamınca bu amaca uygun bir incelemenin yaptırılmış olması gerekir." (Yankı Bağcıoğlu ve Diğerleri, 2014/253, 9 Ocak 2015)

4. "Uygun eğitim" verilmelidir. Personel ve ilk müdahaleyi yapan ekipler, olay yerinde uzman bulunmaması hâlinde elektronik delilleri arayabilecek ve bu delillere elkoyabilecek şekilde uygun eğitimden geçirilmelidir. İlk müdahaleyi yapan görevlinin elektronik delil toplamasının ve/veya bir elektronik cihazda veya dijital depolama ortamında tutulan orijinal verilere erişmesinin gerekli olduğu istisnai durumlarda, ilk müdahaleyi yapan görevlinin bunu düzgün bir şekilde yapabilecek ve yaptığı işlemlerin uygunluğunu ve sonuçlarını açıklayabilecek şekilde eğitim alması gerekmektedir.

5. "Kanunilik" – dosyadan sorumlu memur ve kolluk kuvvetleri; yasalara, hukukun genel ilkelerine ve usûl ilkeleri ile yukarıda listelenen ilkelere uyulmasının sağlanmasından sorumludur. Söz konusu durum, elektronik delillerin bulundurulması ve bunlara erişim açısından da geçerlidir.

5. Önemli siber suç ve siber ortamda gerçekleştirilen geleneksel suç türleri

5.1. Siber saldırı – Soruşturmada dikkat edilecek hususlar

Siber suçlular, bir veya daha fazla bilgisayarı kullanarak bir veya birden fazla bilgisayara ya da bir bilgisayar ağına saldırı başlatabilir. Bir siber saldırı, bir bilgisayarın işlevselliğini bozabilir veya azaltabilir, hukuka aykırı biçimde veri elde edebilir ve/veya bilgisayar(lar)ı başka siber saldırılar düzenlemek için bir saldırı "başlatma noktası" olarak kullanabilir.

Bu kapsamda, bir bilişim sistemine hukuka aykırı olarak girme (TCK m. 243), bir bilişim sisteminde kötü amaçlı yazılım kullanımı (TCK m. 245/A) ve sistemin engellenmesi (TCK m. 244) saldırıları olmak üzere üç temel siber saldırı türü bulunmaktadır. Diğer saldırı türleri, siber ortamda gerçekleştirilen geleneksel suçlar olarak adlandırılmaktadır, zira bu tür suç eylemlerinin gerçekleştirilmesinde, saldırı **hem** başlangıç noktası **hem de** konusu açısından bir bilgisayarın varlığını gerektirmek zorunda değildir.

Siber saldırılar genellikle teknik bir altyapı gerektirir ve bu teknik altyapı suç ihbarı alınırken iki temel sebepten dolayı göz önünde bulundurulmalıdır:

- Söz konusu altyapının ortadan kaldırılması, başka siber saldırıları önleyebilir veya azaltabilir,
- Söz konusu altyapı, soruşturmada kullanılabilecek ve saldırının nasıl gerçekleştiğini gösterecek veya bir kişi veya kuruluşla ilişkilendirilmesini sağlayacak deliller barındırabilir.

Aşağıdaki paragraflarda, yaygın olarak bilinen siber saldırıların nasıl başlatıldığına dair yöntemler sunulmakta ve potansiyel altyapılar açıklanmaktadır. Bu bileşenlerden bazılarının, saldırıların anonim olmasını sağladığı da bilinmektedir.

Örneğin;

- **IP adresleri,** cihazlar ağlara ve internete bağlandığında atanır ve bu **adresler** cihazın tespit edilmesini sağlayabilir.
- Proxy IP adresleri, sanal özel ağ (VPN) ve Onion Router (TOR) gibi kaynaklar, **IP adreslerini yetkililerden gizlemek veya saklamak** için kullanılır.
- Kullanıcıların İnternet Kaynaklarını tanımlamasını sağlayan Alan Adı Sistemi (DNS) ve alan adları[7] kötüye kullanılabilir ve siber suçların işlenmesinde kullanılabilir.
- Saldırganlar genellikle, mağdurun bilgisayarlarına yüklenen kötü amaçlı yazılımlarla dolaylı olarak iletişim kurmak ve virüs bulaşmış birçok cihazı aynı anda kontrol etmek için, saldırıları **komuta ve kontrol sunucularına** bağlar. Komuta ve kontrol sunucuları siber suçlular tarafından kiralanmış, satın alınmış veya onlar tarafından hukuka aykırı olarak kontrol ediliyor olabilir.
- Bir suçlunun veya kuruluşun kontrolü altındaki bir dizi virüslü bilgisayar **botnet** olarak adlandırılmaktadır. Bir botnetin büyüklüğü birkaç bilgisayardan üslü sayılara kadar değişebilmektedir. Bazı botnetlerin milyonlarca virüslü cihazdan oluştuğu bildirilmektedir.[8] Botnetler genellikle 'zombi bilgisayarlar' olarak adlandırılmaktadır. Kötü amaçlı yazılım botnet içindeki her bilgisayara veya cihaza bulaşmış olduğundan, bunların her biri delil mevcudiyeti açısından dikkate alınmalı ve münferit bir olay yeri olarak değerlendirilmelidir.

5.1.1. Siber saldırılarda teknik soruşturmalar

Siber saldırılarla ilgili soruşturmalarda, delillerin nerede depolanmış olabileceği düşünülmelidir. Bu delillere elkoyulması saldırganların tespit edilmesine yardımcı olmak ve şüphelilerin tespit edildiği durumlarda da kovuşturmaya kıymetli deliller sağlamak açısından önemli olabilir. Türkiye dışında depolanan deliller için, cumhuriyet savcıları ve kolluk kuvvetleri, istihbarat amaçlı veya delil olarak kullanılacak materyallerin elde edilmesi için bu kılavuzun 10. Bölümünde açıklanan kaynakları kullanmalıdır.

Teknik soruşturmalar, sistem kütüklerinin, güvenlik duvarı kütüklerinin, izinsiz

7 https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/
8 https://www.zdnet.com/article/a-decade-of-malware-top-botnets-of-the-2010s/

giriş önleme sistemi kütüklerinin ve yapılan işlemleri gösterecek ve suçluların bir sisteme veya cihaza nasıl saldırdığına dair delil sağlayacak diğer kayıtların (bunlarla sınırlı olmamak üzere) analizini içermelidir. Siber saldırı yöntemleri arasında, saldırıdan önce yapılan keşifler de yer almaktadır. Kütük dosyalarının analizi, bu incelemeyi yapmak için normal adli bilişim süreçlerinin yanı sıra uzmanlaşmış teknik programlar da kullanan adli bilişim uzmanları tarafından yapılabilir.

Kötü amaçlı yazılımlarla veya bir bilgisayar sistemine hukuka aykırı olarak girilmesiyle ilgili elektronik delil barındırdığından şüphelenilen canlı bir dijital cihaza elkoyulması hâlinde, canlı adli bilişimin göz önünde bulundurulması oldukça önemlidir. Söz konusu durumlarda, bilgisayarlarda devam etmekte olan ve cihaz kapatıldığında kaydedilmeyecek veya kayıt altına alınmayacak canlı süreçlerin sayısına ilişkin veriler elde edilmelidir. Bu gibi durumlarda, canlı makinelerin adli bilişim görüntülerinin alınması için bir uzmana talimat verilmesi düşünülmelidir.

Kötü amaçlı yazılımlarla ilgili soruşturmalarda, virüsün nasıl bulaştığının ve veri yükünün (kötü amaçlı kodun) neler yapabileceğinin bir uzmana açıklattırılması genellikle faydalı olmaktadır. Çoğu durumda bu uzmanlar, kötü amaçlı yazılımın ne yapmak üzere tasarlandığını mahkemeye bildirmek üzere kontrollü bir şekilde kötü amaçlı yazılım bulaştırdıkları bilgisayarları ve sanal bilgisayarları kullanacaklardır. Kötü amaçlı yazılım soruşturmalarında uzmanlaşma özel bir beceri gerektirir ve adli bilişim görevlileri bu özel uzmanlık alanında delil elde edemeyebilir. Daha sağlam ve güvenilir delillerin elde edilmesi için TK-CERT'den (Ulusal Siber Olaylara Müdahale Merkezi/USOM), akademik camiadan veya başka yerlerden gelecek uzmanlara ihtiyaç duyulabilir.

Soruşturmayı yürüten kişilerin, kötü amaçlı yazılımların genellikle "hash değerleri" aracılığıyla tespit edildiğini ve kötü amaçlı yazılımları yazan kişilerin genellikle kod içerisinde takma adlar, ilişkili çevrimiçi kaynaklar (alan adı hizmetlerini kullanan komuta ve kontrol sunucuları gibi) veya anonim e-posta adresleri içeren izler bıraktığını dikkate alması gerekir. Söz konusu durumlarda bu izlerin tespit edilmesi ve soruşturmanın derinleştirilmesi oldukça önemlidir. Uzmanlardan faydalanmak ve açık kaynaklı istihbarat çalışması yürütmek, genellikle başka bir yerde (komuta ve kontrol sunucuları gibi) bulunan kötü amaçlı yazılımla bağlantılı delillerin aranmasını ve ele geçirilmesini sağlayarak soruşturma süreçlerini destekleyecektir.

5.1.2. Siber saldırılarda mali soruşturmalar

Dolandırıcılık ve mali kayıpların söz konusu olduğu durumlarda, polis ve cumhuriyet savcıları mümkün olan en kısa sürede paralel bir mali soruşturma yürütmeye başlamalıdır. Bu, çalınan fonların transfer öncesi ve sonrasında dondurulmasına yardımcı olacak ve "para akışının takip edildiği" soruşturmaların yürütülmesini mümkün kılacaktır.

Öncelikle, mağdur tarafından dolandırıcının hesabına para transferi yapılmışsa, soruşturmayı yürüten makamlar parayı dondurmak için mümkün olan tüm adımları ivedilikle atmalıdır. Geleneksel bankacılık sistemlerinin kullanıldığı transferde, bu adımın transfer işleminin gerçekleşmesinden sonraki 24 saat içinde başarılı olma olasılığı daha yüksektir.

Suçlular genellikle bu finansal transferleri, fonları daha sonra kendi kontrolleri altındaki başka banka hesaplarına aktararak ilave kara para aklama süreçlerini işletecek şekilde planlarlar. Soruşturmayı yürüten kişilerin göz önünde bulundurması gereken bir diğer yöntem, parayı para transfer hizmetleri aracılığıyla suçlulara göndermeden önce ATM'lerden nakde çevirecek 'para katırı ağlarının' (mule networks) kullanılmasıdır.

Soruşturmalar, önemli ölçüde zaman ve kaynak gerektiren "para akışının takip edildiği" süreçleri kapsayabilir ve fonlara elkoyulamadan sona erebilir. Yine de soruşturmalar, başarı ihtimalini artırmak için mümkün olan en erken aşamada başlatılmalıdır.

Bir başka soruşturma taktiği, gizli görev becerileri kullanarak ve/veya mağdurları görevlendirerek kontrollü transfer veya para teslimatları ayarlamak için şüpheliyle gizlice iletişim kurulmasıdır. Bu taktik, soruşturmalarda belli ölçüde başarılı olsa da başarılı olma olasılığı her soruşturmanın kendi özel koşullarına bağlıdır. Şantaj vakalarında, istenilen paranın miktarını düşürmek için yapılan pazarlıklar, genellikle soruşturmayı yürütenlere daha fazla bilgi sağlamakta ve diğer soruşturma seçeneklerini değerlendirmek için zaman kazandırabilmektedir.

Para akışının takip edildiği soruşturma adımları her zaman önemlidir, bu yüzden dolandırıcının kimliğini ve/veya suç gelirlerinin yerini tespit edebilecek bilgilerin titizlikle ele alınması gerekmektedir. Bu soruşturmalar, paranın finansal kurumdan ne zaman gönderildiğinin veya alındığının ortaya

çıkartılması için fırsat yaratabilir ve şüphelilerin veya suç ortaklarının tespit edilip tutuklanmasını sağlayabilir.

Sanal ödeme sistemlerinin ve kripto para birimlerinin kullanıldığı suçlar ve durumlar için bu kılavuzun 8. Bölümüne bakınız.

5.2. Siber suç ve siber ortamda gerçekleştirilen geleneksel suç türleri

5.2.1. DDoS

Dağıtık hizmet engelleme (DDoS) saldırıları, çevrimiçi bir hizmete, sunucuya, web sitesine veya ağa yönelik düzenlenen ve internet trafiğini bu kaynağa yönlendirerek kapasitesinin üzerinde yoğunluk oluşturmayı hedefleyen siber saldırılardır.

Saldırgan, saldırıyı yönlendirmek için kullanılacak bir komuta ve kontrol sunucusu tarafından kontrol edilen bilgisayarlardan oluşan bir botnete ihtiyaç duyar. Suçlu, saldırı noktasını (örneğin bir web sitesi veya IP adresi) belirler ve botnetten kaynağa doğru veri trafiğini başlatır. Trafik yoğunluğu nedeniyle, hedeflenen sistem aşırı veri yüklenmesine maruz kalır ve meşru kullanıcılar tarafından kullanılamaz hâle gelir. Bu durum, internet üzerinden satış yapanlar için ciddi mali kayıplara neden olabilmektedir.

DDoS saldırılarının nedenleri arasında, saldırıyı durdurmak için şantaj yoluyla para talep etme, intikam, hacktivizm (siyasi amaçlı internet saldırısı düzenleme/siber aktivizm) ve devlet destekli saldırılar yer almaktadır. DDoS saldırıları ayrıca, başka bir siber saldırının gerçekleştirilebilmesi için dikkat dağıtma amacıyla da kullanılmaktadır.

Soruşturmada, potansiyel elektronik delillere yönelik aşağıdaki hususlar dikkate alınmalıdır:

- Saldırının başladığı andan itibaren mağdurun web sitesine veya sunucuya ait kütüklerin korunması
- Önceki sunucu kütüklerinin saldırganlar tarafından gerçekleştirilen keşif ve daha küçük çaplı deneme saldırılarını gösterebileceğinin unutulmaması
- Fidye talebi göndermiş olabilecek tüm e-posta hesaplarının korunması

- Faille yapılan her türlü iletişimin kaydedilmesi
- Her türlü ödeme yönteminin detayları.

DDoS ile ilgili risk azaltma önlemleri hakkında Ulusal Siber Olaylara Müdahale Merkezinden (TK-CERT) bilgi alınmalıdır.

5.2.2. Web uygulamalarına yönelik saldırılar

Web uygulamalarına yönelik saldırılar, çevrimiçi bir hizmete, sunucuya, web sitesine veya ağa yönelik gerçekleştirilen ve saldırganların bilgisayar kodundaki bir güvenlik açığını tespit etmeye ve bu açıktan yararlanarak kaynağa hukuka aykırı olarak girmeye çalıştığı siber saldırılardır.

Web uygulamalarına yönelik saldırılarının dört ana türü bulunmaktadır:

- SQL Enjeksiyonu
- Siteler Arası Komut Dosyası Çalıştırma
- Uzaktan Dosya Ekleme
- Siteler Arası İstek Sahteciliği

Çoğu çevrimiçi kaynağın web uygulamalarının, bu uygulamanın çalışmasını ve kullanıcı verilerini almasını ve işlemesini sağlayan bir bilgisayar kodu bulunmaktadır. Alınan veri bir kullanıcı adı ve parola olabileceği gibi, sunucu (veya bilgisayar) tarafından erişilip işlenebilecek bir dosya veya başka bir şey de olabilir. Çoğu durumda, uygulanan bilgisayar kodunda güvenlik açıkları bulunur ve bu güvenlik açıkları, saldırganların bilgisayarın gerçekleştirmesi gereken bir işlem gibi algılayacağı bir formatta veri girişi yapmasını mümkün kılar. Ancak saldırgan veriyi, sunucunun (veya bilgisayarın) gizli alanlarına ve büyük olasılıkla bir ağın ana altyapısına erişim sağlamak için bilgisayar kodunu hukuka aykırı olarak manipüle edecek şekilde hazırlayacaktır.

Bu tür saldırıların altında yatan motivasyon genellikle finansaldır (örneğin finansal kayıtların ve kredi kartı bilgilerinin elde edilmesi). Bununla birlikte web uygulamalarına yönelik saldırılar bilgi edinmek, casusluk yapmak ve kötü amaçlı yazılım yerleştirmek için de kullanılabilmektedir. Web uygulamalarına yönelik saldırıların yol açtığı küresel kayıplar DDoS saldırılarının yol açtığı kayıplardan çok daha fazladır.

Soruşturmada, potansiyel elektronik delillere yönelik aşağıdaki hususlar dikkate alınmalıdır:

- Saldırının başladığı andan itibaren mağdurun web sitesine veya sunucuya ait kütüklerin korunması;
- Önceki sunucu kütüklerinin saldırganlar tarafından gerçekleştirilen keşif ve daha önceki erişim girişimlerini gösterebileceğinin unutulmaması.

Web uygulamalarıyla ilgili önleme ve risk azaltma adımları hakkında Ulusal Siber Olaylara Müdahale Merkezinden (TK- CERT) tavsiye alınmalıdır.

5.2.3. Kötü amaçlı yazılım (malware) saldırıları

Kötü amaçlı yazılım saldırıları, kötü amaçlı yazılımların (zararlı yazılımların) mağdurun sisteminde izinsiz eylemler gerçekleştirdiği, oldukça sık rastlanan siber saldırılardır. Birçok farklı kötü amaçlı yazılım türü bulunmakta olup bu yazılımlar sisteme yönelik çeşitli saldırılar gerçekleştirirler.

Farklı kötü amaçlı yazılım türleri tanımlanırken, bu tanımın genellikle yazılımın içerdiği veri yükünün türünden ziyade, yazılımın bilgisayar sistemine nasıl bulaştığıyla ilgili olduğunun bilinmesi önemlidir.

Örneğin:

- Bilgisayar Virüsü, kendini kopyalayabilen ve diğer programlara veya dosyalara kendini ekleyebilen ve bu işlem sırasında bunlara bulaşabilen bir kod parçasıdır. Kullanıcılar, virüs bulaşmış dosyaları paylaşarak veya ileti ekinde virüs olan e-postaları göndererek farkında olmadan virüsü yayarlar.
- Bilgisayar Solucanı, kendini kopyalayabilen ve kopyalarını kullanıcı etkileşimi olmadan bilgisayardan bilgisayara yayabilen bir kod parçasıdır.
- Truva Atı olarak adlandırılan kötü amaçlı yazılım, meşru bir yazılım gibi görünen ve genellikle sosyal mühendislik yoluyla kullanıcıyı kötü amaçlı yazılımı yüklemesi ve çalıştırması için kandırarak kullanıcı sistemlerine erişim sağlayan bir tür kötü amaçlı yazılımdır.
- Daha birçok başka kötü amaçlı yazılım türü vardır, bunlardan bazıları aşağıda sunulmuştur:

- virüs yükleyiciler (droppers) ve indiriciler (örneğin botnetlerin bir parçası olarak)
- bilgi hırsızları (örneğin tuş kaydediciler (keyloggers), casus yazılımlar)
- özel truva atları (örneğin bankacılık truva atları)
- arka kapılar (örneğin rootkitler)
- dosya/program siliciler (wipers)
- fidye yazılımları.

Kötü amaçlı yazılım kullanımının altında yatan pek çok motivasyon vardır ve bu tarz yazılımlar devlet aktörleri, siber suçlular, hacktivistler (siber aktivistler) ve endüstriyel casusluk yapan kişiler tarafından kullanılmaktadır.

5.2.4. Fidye yazılımı (ransomware)

Fidye yazılımı, veri yükünün bir bilgisayar sistemi veya dijital cihazdaki kullanıcı dosyalarını veya klasör içeriğini kasıtlı olarak şifrelediği bir kötü amaçlı yazılım türüdür. Saldırgan, şifreleme saldırısıyla birlikte bir mesaj göndererek veya bilgisayarda bir açılır pencere (pop-up) oluşturarak, belirli bir hesaba genellikle kripto para birimi cinsinden fidye ödemesi yapılmasını talep eder. Ödemenin alınmasının ardından, saldırganlar dosyaların şifresini çözeceklerini ve erişimi geri yükleyeceklerini veya şifre çözme anahtarını sağlayacaklarını belirtirler. Normalde ödeme yapıldıktan sonra erişim geri yüklenir, ancak fidye ödemesi ufak meblağlardan milyonlarca Türk Lirasına kadar değişebilmektedir.

Bu tür saldırıların farklı çeşitleri vardır. Bunlardan biri, saldırganın yerel, ulusal veya uluslararası bir kolluk kuvveti veya benzeri bir kurum mensubu olduğunu iddia ederek kullanıcının birtakım yasaları ihlâl ettiğini söylemesi ve fidye ödemesinin, ödenmesi gereken bir para cezası gibi sunulmasıdır. Son dönemlerde fidye yazılımları, sistemlere virüs bulaştırmak için ağlardaki çeşitli güvenlik açıklarından yararlanarak veya sosyal mühendislik saldırılarını kullanarak kurumsal ağları hedef almaktadır.

Virüs bulaşmış olduğu, kullanıcının bilgisayar ekranında sadece, kaynağın şifrelendiğini ve ancak talep edilen fidyenin ödenmesi durumunda şifresinin çözülebileceğini belirten bir fidye talebi sayfasının görüntülenmesiyle tespit

edilir. Ödeme her zaman kripto para birimlerinde talep edilir ve bilgisayar korsanlarıyla iletişim genellikle anonim kanallar aracılığıyla gerçekleştirilir. Bu kılavuzun yazıldığı sırada kullanılan kanal, bir P2P (eşdüzeyler arası) anlık mesajlaşma protokolü olan 'Tox Chat' idi.

Fidye yazılımı pazarı 2021'den bu yana giderek daha organize ve profesyonel hâle gelmiş olup, fidye yazılımı suçlarını işlemek için genellikle "Hizmet Olarak Fidye Yazılımı" (veya RaaS) şeklinde adlandırılan bir iş modeli sunmaktadır. Bu iş modeli, siber suçluların ödemelerde pazarlık yapmak veya mağdurlara ödeme yapmalarında yardımcı olmak gibi bağımsız hizmetler sunmaya başlamasına ve fidye ödemelerini hızlandırmak ve şifrelendirilen sistemlerin veya verilerin kurtarılmasına yardımcı olmak için 7/24 yardım merkezi hizmetleri vermeye başlamasına yol açmıştır.[9]

Saldırganlar bu hizmetlere yönelik talebi artırmak amacıyla çalışma yöntemlerini de geliştirmiş ve saldırıya maruz kalan sistemlerdeki gizli verilerin büyük bir kısmını kopyalamaya başlamıştır. Mağdurun talep edilen fidyeyi ödemeyi reddetmesi durumunda, saldırganlar gizli verileri internetin herkese açık alanlarında yayınlayarak itibar kaybına neden olmakta ya da tehdidi artırmak veya kişisel bilgileri saldırıya uğrayan sistemde saklanan kişilerden (örneğin müşteriler ve tıbbi hastalar) taleplerde bulunmak için veri sahipleriyle iletişime geçmektedir.

Soruşturma esnasında, kötü amaçlı yazılım bulaştığına dair belirti bulunan tüm cihazların izole edilmesi ve özel inceleme amacıyla korunması gerektiği unutulmamalıdır. Yapılacak incelemede, bu kılavuzun 5.1.1. Bölümünde yer alan tavsiyeler dikkate alınmalıdır. Soruşturmayla ilgili bir diğer husus da mağdurun talep edilen fidyeyi ödeyip ödemeyeceğidir. Bu, tercih edilmeyen bir seçenek olsa da işletme (mağdur), talep edilen fidyeyi ödenmenin, bir sistemin yeniden inşa edilmesinden veya kaynağın şifrelenmiş veriler olmadan çalışmaya devam etmesinden daha düşük maliyetli olacağını düşünebilir. Kripto para birimi ile yapılan tüm ödemeler, soruşturmada blokzinciri (blockchain) teknolojisi kullanılarak 'para akışının takip edilmesi' seçeneğinin kullanılabilmesini mümkün kılmaktadır.

Soruşturmayı yürütenler, şifre çözme anahtarlarına "No More Ransom"

9 https://rm.coe.int/t-cy-2022-14-guidancenote-ransomware-v4adopted/1680a9355e

(Fidyeye Son) sitesi gibi kaynaklar üzerinden erişilebileceğini unutmamalıdır[10]. Araştırılabilecek diğer hususlar arasında, bulaşma yönteminin (genellikle bir oltalama e-postası) incelenmesi yoluyla siber saldırının kaynağının sorgulanması, saldırganlarla iletişim kurulması ve saldırganların taleplerini güçlendirebilecek herhangi bir veriye erişip erişmediğinin belirlenmesi için sistemlerin detaylı bir şekilde incelenmesi yer almaktadır.

Soruşturma çerçevesinde veya adli bilişim analizi yoluyla, bulaşmanın kapsamı, büyüklüğü ve potansiyel erişim alanının belirlenmesi için inceleme yapılmalıdır. Cihazların türünün ve sayısının tespit edilmesi önemli bir adımdır. Kötü amaçlı fidye yazılımının türü ve sürümünün yanı sıra, kötü amaçlı yazılımın cihazlara ve ağlara nasıl sızdığı da tespit edilmelidir.

Genellikle suçlulara ve delillere ulaşmanın mümkün olmadığı ülkelerde (Rusya Federasyonu gibi), fidye yazılımı saldırıları ile ilgili yürütülen soruşturmalarda şüphelilere ve delillere ulaşılabilmektedir. Ulusal ve uluslararası paydaşlarla (Europol ve Interpol) istihbarat paylaşımı, soruşturma ve kovuşturmanın artık başarılı bir şekilde tamamlanamayacağı bir aşamaya ulaşıldığında bile her zaman göz önünde bulundurulmalıdır.

Önleme ve destek tedbirleri ile ilgili daha fazla bilgi Ulusal Siber Olaylara Müdahale Merkezinden (TK-CERT) alınabilir.

5.3. Veri ihlâlleri

Veri ihlâli; hassas, korunan veya gizli verilerin izinsiz bir kişi tarafından kopyalandığı, iletildiği, görüntülendiği, çalındığı veya kullanıldığı, bir bilgisayar sistemine veya cihaza yönelik bir güvenlik ihlâlidir. Güvenlik ihlâli, bir veri sisteminin kimlik doğrulama ve yetkilendirmeye yönelik güvenlik protokollerini geçebilen kişiler tarafından kaynaklara hedefli bir şekilde izinsiz girilmesi örneğindeki gibi kasıtlı; veya hassas bilgilerin işlenmesi süreçlerinde bireylerin, işletmelerin veya devlet dairelerinin yetersiz veya dikkatsiz davranması yüzünden ortaya çıkan veri sızıntıları veya veri kaçakları örneğindeki gibi kasıt dışı olabilir.

Veri ihlâllerini ele alırken göz önünde bulundurulması gereken yasal çerçeve aşağıdaki gibidir:

10 https://www.nomoreransom.org

a) Saldırganın bir bilgisayar sistemindeki verilere hukuka aykırı olarak erişim sağlaması, yasal çerçeveye göre TCK Madde 243 uyarınca suç teşkil etmektedir.

b) Kişisel verilerden sorumlu kişi veya kurumların verileri işlerken ihmâl veya dikkatsizliği sebebiyle veri sızıntısı veya veri kaybı olması hâlinde, veri sorumlusu ve/veya veri işleyen, Kişisel Verilerin Korunması Kanunu uyarınca Kişisel Verileri Koruma Kurumu tarafından para cezası uygulanabilir.

c) Birçok veri ihlâli vakasında, her iki senaryo da geçerli olmaktadır.

Bu tür ihbarlar alındığında, soruşturmada Kişisel Verileri Koruma Kurumu gibi Kişisel Verilerin Korunmasına Yönelik Düzenlemelerden sorumlu makamların da bilgilendirilmesinin gerekli olup olmadığına karar vermek için uygun tavsiyelerin alınması gerekebilir.

5.3.1. İç tehdit (insider-threat) (bilgisayar açısından)

İç tehdit, güvenlik riski oluşturan ve genellikle hedef alınan kurumun içinde bulunan bir kişidir. Tipik olarak bu tür tehditler, bir kurumun bilgisayar sistemindeki veya ağındaki hassas bilgilere veya ayrıcalıklı hesaplara erişimi olan mevcut ya da eski çalışanlardan ve personelden gelmektedir.

İç tehdit, bilgisini veya erişimini bir veri ihlâli gerçekleştirmek için kullanabilir, ancak güvenlik tehdidi sadece böyle bir saldırıyla sınırlı değildir. Bunun yanı sıra, mali kayıp yaşanması ve/veya bilgisayar hizmetlerinin kesintiye uğraması amacıyla bir kişi veya kuruma yönelik izinsiz değişikliklere ve silinmelere sebep olabilir veya hizmet engelleme saldırıları başlatabilirler.

İç tehditlerin genellikle organize suç grupları tarafından teşebbüslerini geliştirmek amacıyla kurum içine kasıtlı olarak yerleştirilebildiği ve/veya bu tür gruplar tarafından suç girişiminin yararına hareket etmeleri için kendilerine rüşvet verilebildiği unutulmamalıdır.

Kolluk kuvvetleri ve cumhuriyet savcıları bu saldırılardan bazılarında, ısmarlama kötü amaçlı yazılımların geliştirilmesi ve çevrimiçi hizmetlere arka-kapı erişimi sağlanması gibi karmaşık teknik becerilerin kullanılması gerektiğini unutmamalıdır.

5.3.2. Güvenlik açıklarından yararlanma

Güvenlik açığı, bilgisayarlarda ve teknolojide devamlı olarak bulunan bir sorun, kusur, eksiklik veya yazılım hatasıdır. Güvenlik açıkları sistem için zararlı olmasa da programcılar ve bilgisayar kodlayıcıları çevrimiçi bir hizmet oluşturup var olan açıkları fark etmediğinde ortaya çıkabilmektedir.

Güvenlik açıkları işletim sistemlerinde, uygulamalarda, bilgisayar programlarında ve bilgisayar sistemlerinin donanımlarında bulunur. Zaman zaman güvenlik açıkları tespit edilir ve riski azaltmak için yamalar veya güncellemeler oluşturulur. Yama ve güncellemeler yapıldığında, yamaları ve güncellemeleri kullanan sistemlerde artık güvenlik açığı kalmamış olur. Ancak yeterince hızlı yama ve güncellenme yapmayan hizmetler, yama veya güncellemenin yayınlanmasıyla birlikte suçluların haberdar olabileceği, bilinen güvenlik açıklarına sahip olacaktır.

Bilgi ve İletişim Teknolojisi alanında çalışan güvenlik mühendisleri, güvenliği sağlamak amacıyla sistemleri incelemek için düzenli olarak güvenlik açığı tarayıcıları kullanır. Saldırganlar da saldırı için potansiyel mağdurlarını belirlerken, güvenlik açığı tarayıcıları ve güvenlik açığı veri tabanları da dâhil olmak üzere, aynı kaynakları kullanmaktadır.

Saldırganlar, güvenlik açığını ortaya çıkarmak ve bir bilgisayar sistemine hukuka aykırı olarak erişim sağlamak için kullanılabilecek açıklardan yararlanma yazılımları geliştirmektedir. Açıklardan yararlanma yazılımları arasında kötü amaçlı yazılımlar, bilgisayar kodları (komut dizisi) ve açık kaynaklı yazılım kitleri yer almaktadır.

Bu tür saldırılara örnek olarak aşağıdakiler verilebilir:

- SQL Enjeksiyonu saldırıları
- Siteler Arası Komut Dosyası Çalıştırma
- Siteler Arası İstek Sahteciliği saldırıları
- Hatalı güvenlik yapılandırmaları.

5.4. Sosyal Mühendislik Saldırıları – e-posta yoluyla

Bir mağduru hassas verileri ifşa etmesi veya bir bilgisayar sisteminin güvenliğini tehlikeye atacak bir eylemde bulunması için kandırmak amacıyla

sosyal mühendislik becerilerini kullanan birçok siber suç saldırısı türü ve tanımı bulunmaktadır.

Sosyal mühendislik, teknik bir güvenlik açığından ziyade insan psikolojisinden yararlanan bir beceri veya sanat olarak kabul edilmektedir ve saldırganların sistemlere ve verilere erişmesine olanak tanımaktadır. Zira kullanıcı, saldırganın talimatıyla görünüşte masum bir görevi yerine getirirken aslında farkında olmadan erişime izin vermiş olur.

Pek çok sosyal mühendislik saldırısı e-posta yoluyla gerçekleştirilmektedir, ancak genellikle sosyal medya, yüz yüze iletişim veya ses teknikleri yoluyla kullanıcının kandırılmasıyla gerçekleşen dolandırıcılık ve siber saldırılar gibi örnekler de vardır.

5.4.1. Oltalama (Phishing)

Oltalama, başka görünümdeki bir e-posta veya elektronik haberleşme yöntemi kullanarak mesajın bir kişiden (arkadaşı, meslektaşı veya akrabası gibi) veya bir finans kurumu, banka, çevrimiçi alışveriş sitesi veya başka bir web kaynağı gibi gerçek bir hizmet sağlayıcısından geldiğine inanması için alıcıya gönderilen ve mağduru, gömülü bir bağlantıya tıklaması veya bir eki indirmesi için kandıran bir sosyal mühendislik saldırısıdır.

Oltalama e-postaları görünürde genellikle profesyonel olsa da çoğu zaman belirli bir hedef gözetmezler ve e-posta adresleri toplanmış olan pek çok alıcıya gönderilirler.

"Olta" benzetmesinin nedeni, bu saldırı yönteminde genellikle geniş bir hedef gruba birkaç "yemli kancanın" atılarak yemin yutulmasının beklenmesidir. Yemin yutulma anı, kullanıcının kandırıldığı ve görünüşte masum olan bir talimatı yerine getirdiği andır.

Tıklanan gömülü bağlantılar genellikle mağduru, kullanıcılardan kullanıcı adlarını ve parolalarını girmelerini isteyen sahte veya dolandırıcı web sitelerine yönlendirir ve bu kullanıcı adları ve parolalar daha sonra suçlular tarafından toplanarak dolandırıcılık amaçlı kullanılır. E-posta eklerinde genellikle bilgisayarın güvenlik sistemini tehlikeye atan, gömülü kötü amaçlı yazılımlar (veya kötü amaçlı yazılım yükleyicileri) yer alır.

Suçlular, kullanıcının bağlandığı ve kimlik doğrulama bilgilerini girdiği, güvenlik zafiyeti oluşturulmuş web sitelerini ve web sunucularının yer aldığı "oltalama

kitlerini" satın alabilmekte veya söz konusu kitleri kendileri oluşturabilmektedir. Kısa bir süre açık kalan bu siteler, siber güvenlik profesyonellerinin, suçluların faaliyetlerini engellemesini önlemek amacıyla oluşturulmaktadır.

Alan adı hizmetleri (DNS) ve suçluların e-posta adresleri, dolandırıcılığı pekiştirmek için genellikle gizlenir ve sahte web siteleri, çoğu zaman gerçek çevrimiçi hizmetlerin profesyonel kopyaları görünümündedir.

Oltalama e-postalarıyla ilgili bir suç ihbarı alındığında, yürütülecek soruşturmada ulusal ve uluslararası yasal çerçevelerde nelere izin verildiği göz önünde bulundurmalıdır. Pek çok yargı sisteminde, oltalama amaçlı e-posta gönderilmesi suç olarak tanımlanmamaktadır ve siber suç ihbarının yapılması için, mağdurun ihbar öncesinde dolandırılmış veya veri ihlâline maruz kalmış olması gerekebilmektedir. Cumhuriyet savcısı, uluslararası bilgi talebinde bulunurken, Türkiye ile talebin iletildiği ülke arasındaki mütekabiliyeti dikkate almalıdır.

Soruşturmada, alan adı hizmetinin kullanılmış olabileceği ve bu hizmetin genellikle ödeme gerektiren bir hizmet olduğu unutulmamalıdır. Bir web sitesinin kaydedilmesi için (bu, suç amaçlı kullanılan bir web sitesi olsa bile), sunucunun tanımlanabilir bir alan adıyla internete bağlanması gerekmektedir. Hizmet sağlayıcıya yönelik soruşturma, Whois Veri Tabanları aracılığıyla ve akabinde, birçoğu kolluk kuvveti portallarına sahip olan hizmet sağlayıcılara iletilen talepler yoluyla mümkündür.

E-postaların ve altyapıların soruşturulmasında, 7/24 Tek İrtibat Noktasından destek sağlanabilir – Bkz. Bölüm 6.3 ve Bölüm 10.

5.4.2. Hedefli oltalama (Spear Phishing)

Hedefli oltalama e-postaları ve iletişimleri, daha sofistike oltalama saldırılarıdır. Bu mesajlar ve iletişimler genellikle profesyonel görünümdedir ve alıcıları hedeflenmiş kişilerdir; dolayısıyla belirli bir kişiye, kuruma veya işletmeye gönderilirler. Saldırganlar, alıcının iletişimde yer alan gömülü bir bağlantıya veya eke tıklama ihtimalini artıracak bazı ek ön araştırmalar da yapmış olabilir.

Hedefli oltalama saldırılarında da oltalama saldırılarında kullanılan benzer altyapılar kullanılmaktadır. Saldırganın mesajlarında ek olarak bir de sosyal mühendislik becerileri kullanması nedeniyle, hedefli oltalama saldırılarının başarılı olma olasılığı daha yüksektir.

Hedefli oltalama mesajları gönderen saldırganlar, mağdurlarla iletişimlerinde genellikle farklı haberleşme yöntemleri (e-postaya ek olarak) kullanmaktadır. Tüm bu haberleşme yöntemlerinin, 7/24 Tek İrtibat Noktasından alınacak destek yoluyla daha derinlemesine soruşturulması gerekmektedir – Bkz. Bölüm 6.3 ve Bölüm 10.

5.4.3. Balina Avı (Whaling)

Balina avı, genellikle kurumsal dünyadaki üst düzey yöneticilere yönelik, oldukça hedefli bir oltalama saldırısıdır. Ön araştırma ve sosyal mühendislik yöntemleri kullanılarak yapılan bu saldırılar sayesinde mağdurun daha yüksek miktarlarda para transferi gerçekleştirmesi amaçlanmaktadır.

İlk iletişim e-posta veya çevrimiçi haberleşme yoluyla gerçekleşebilir, ancak dolandırıcılığı ilerletmek için genellikle fiziksel ve sesli etkileşimler da kullanılmaktadır. Balina avı e-postaları genellikle oltalama ve hedefli oltalama saldırılarında görülen e-postalardan daha sofistikedir ve aşağıda belirtilen özelliklere sahiptir:

- Kişi veya kurum hakkında kişisel bilgilerin kullanılması
- Aciliyet hissi yaratılarak dolandırıcılığın inandırıcı hale getirilmesi
- Mağdurun, dış dünyayla iletişim kurmasını engelleyecek bir durumun yaratılması, örneğin konunun güvenlik nedeniyle gizli tutulmasının gerekmesi
- Mesajların, iş dünyasında kullanılan terimlerle ve iş dünyası diliyle yazılması.

5.4.4. Şirket e-postası dolandırıcılığı (ŞED)/Genel Müdür dolandırıcılığı (CEO Dolandırıcılığı)

Şirket e-postası dolandırıcılığı/CEO dolandırıcılığı, genellikle kurumsal dünyada mali işlemlerden sorumlu çalışanlara ve yöneticilere yönelik, oldukça hedefli bir sosyal mühendislik saldırısıdır. Bununla birlikte örneklere bakıldığında, bu tarz saldırıların çoğunlukla büyük çaplı finansal işlemler yapan kişilere yönelik düzenlendiği görülmektedir.

Şirket e-postası dolandırıcılığı/CEO dolandırıcılığı, birçok yönden balina avı gibi oltalama saldırılarına benzese de bazen saldırganların, tedarikçi ile müşterisi

arasındaki yazışmaları görebilmek için bir e-posta hesabına hukuka aykırı erişim elde etmesi gerekmektedir. Saldırganlar böylece mağdura, işlem için kullanılacak banka hesabının değiştirilmesi gerektiğini belirten bir e-posta gönderebilir ve bu yazışmalara genellikle ödemenin acil olduğuna dair bir mesaj eklenir. Mesajı gönderen kişi, ödemenin yapılması talimatını daha inandırıcı kılmak için genellikle üst düzey bir yönetici (CEO seviyesi) veya benzeri bir kişi olduğunu iddia eder.

Bu tür suçların dünya çapındaki finansal etkileri sebebiyle, bu saldırılar en önemli siber saldırı türlerinden kabul edilmektedir.

Suçlunun banka hesap detaylarını içeren mesajı gönderen e-posta hesabının kaynağının soruşturulmasının yanı sıra, bu soruşturmanın zaman açısından en kritik olan adımı, söz konusu saldırıyla bağlantılı finansal işlemlerin acilen dondurulmasıdır. Soruşturmayı yürütenler, fonların başka yerlere transfer edilmesini durdurmak için Türkiye ve başka ülkelerdeki bankalar veya finansal kuruluşlarla iletişime geçmek için her türlü yöntemi denemelidir. Bu fonlar genellikle ilk 24 saat içinde başarılı bir şekilde kurtarılabilirken, bu sürenin dolmasının ardından soruşturma, başarı oranının daha düşük olduğu 'para akışının takip edilmesi' sürecine dayanacaktır. MASAK ve Emniyet Genel Müdürlüğü'ne bağlı Mali Suçlarla Mücadele Şube Müdürlüğü gibi kurumların her türlü dondurma işlemini destekleyeceği unutulmamalıdır.

5.5. Sosyal mühendislik saldırıları – Diğer saldırılar

Sosyal mühendislik saldırılarıyla en iyi mücadele yöntemi; önleme, farkındalık ve eğitimdir. Bu suçların çözülmesi, genellikle karmaşık süreçler gerektirir ve soruşturmayı yürütenlerin göz önünde bulundurması gereken uluslararası boyutları da bulunmaktadır.

Dolandırıcılığın gerçekleşmesi için, genellikle çevrimiçi olarak veya başka bir para transferi sistemi aracılığıyla (sanal ödeme sistemleri veya kripto para birimleri de dâhil) bir ödeme yapılmış olması gerekir. Her ne kadar kovuşturmalar suça teşebbüs ve suç komplosu gibi yasal çerçevelere dayanabilse de dolandırıcılık fiili tamamlanmadan önce, ceza kanunu kapsamında suç işlendiğinin kanıtlanması genellikle zordur.

Çoğu sosyal mühendislik saldırısı, ancak mağdur maddi kayba uğradıktan sonra kolluk kuvvetlerine ve cumhuriyet savcılarına bildirilmektedir. Yukarıda yer alan Bölüm 5.4.4'teki finansal adımlara bakınız.

Mali soruşturmanın yanı sıra, soruşturma stratejisi, dolandırıcılığın gerçekleştirilmesinde kullanılan sosyal medya platformundan, e-postalardan veya diğer sistemlerden elde edilen iletişim verilerine dayanacaktır. Söz konusu strateji, e-posta başlıklarının soruşturulmasını veya çok uluslu hizmet sağlayıcılardan bilgi alınması amacıyla başvuru yapılmasını gerektirebilir. İletişim verilerine yönelik soruşturmalar ve uluslararası delil talepleri, 7/24 Tek İrtibat Noktasının desteğiyle geliştirilebilir. Konuyla ilgili daha fazla bilgi için bu kılavuzun 10. Bölümüne bakınız.

Bu suçlar çoğunlukla Batı Afrika menşelidir ve bu bölgedeki kolluk kuvvetlerinin, ön ödeme dolandırıcılığı ve sanal flört dolandırıcılığı gibi sosyal mühendislik dolandırıcılıklarına son derece aşina olan özel soruşturma ekipleri bulunmaktadır. Türkiye'deki cumhuriyet savcıları ve polis, uygun iş birliği ve yardımlaşma kanalları aracılığıyla (Interpol, Polisler Arası İşbirliği ve Karşılıklı Adli Yardım gibi) bu kaynaklarla erkenden irtibata geçilmesini değerlendirmelidir.

5.5.1. Ön ödeme dolandırıcılığı

Ön ödeme dolandırıcılığı, en yaygın sosyal mühendislik saldırılarından biridir. Bu dolandırıcılık yönteminde genellikle dolandırıcı, büyük miktarda para elde etmek için kullanılacağını iddia ettiği küçük bir ön ödeme karşılığında, mağdura büyük meblağdan önemli bir pay vereceğini vadeder. Mağdurun ödemeyi yapması durumunda, dolandırıcı ya mağdurun ödemesi için bir dizi ilâve ücret icat eder ya da doğrudan ortadan kaybolur.

5.5.2. Sanal flört dolandırıcılığı

Sanal flört dolandırıcılığı, mağdura karşı romantik niyetler besliyormuş gibi davranmayı, mağdurun sevgisini kazanmayı ve daha sonra bu iyi niyeti kullanarak mağdurun sahte tavırlar sergileyen dolandırıcıya para göndermesini veya mağdurun başka dolandırıcılıklara maruz kalmasını sağlayan bir sosyal mühendislik saldırısıdır. Dolandırıcılık eylemleri arasında, mağdurun parasına, banka hesaplarına, kredi kartlarına, pasaportlarına, e-posta hesaplarına veya kimlik belgelerine erişilmesi ve/veya mağdurun saldırgan adına mali dolandırıcılık yapmaya zorlanması yer almaktadır.

Bu suçlar genellikle aynı anda birden fazla mağdurdan para almak için birlikte çalışan organize suç çeteleri tarafından işlenir.

Sosyal mühendislik saldırılarında ve özellikle sanal flört dolandırıcılığında göz önünde bulundurulması gereken bir husus, mağdurların çoğu zaman, 'ilişki' yaşadıkları kişinin bir dolandırıcı olduğuna inanmakta zorlanmasıdır. Soruşturma stratejisi, kolluk kuvvetlerinin dolandırıcıyla müzakere etmesini ve etkileşim kurmasını gerekli kılabilir, ancak mağdurla ne kadar bilgi paylaşılacağı konusuna dikkat edilmelidir. Saldırganın mağduru (sonradan tekrar kendisiyle iletişime geçerek) dürüst bir kişi olduğuna ve ortada bir dolandırıcılık olmadığına ikna ettiği birçok örnek bulunmaktadır. Dolayısıyla şüpheli(ler), mağdurun bizzat kendisi tarafından, haklarında polis soruşturması yürütüldüğü konusunda uyarılabilmektedir.

5.6. Çevrimiçi dolandırıcılık

İnternet üzerinden gerçekleştirilen, genellikle siber suç dolandırıcılığı veya düzenbazlığı olarak adlandırılan ve saldırganların dolandırıcılık ve sosyal mühendislik yöntemlerini birlikte kullanarak mağduru, suçluların kontrolü altındaki finansal hesaplara gönüllü olarak para veya varlık aktarması için kandırdığı pek çok internet dolandırıcılığı türü bulunmaktadır.

İnternet dolandırıcılığı kısmen veya tamamen internet hizmetlerinin kullanımına dayalı olabilse de finansal işlemlerin gerçekleştirilebilmesi tamamıyla teknoloji kullanımını gerektirmektedir.

Bu paragraflarda, en yaygın İnternet Dolandırıcılığı türlerine ilişkin bazı açıklamalar yer almaktadır ve bu dolandırıcılık türlerinin soruşturulmasında, bu kılavuzda Bölüm 5.4 ve 5.5'te yer alan soruşturma seçeneklerine ilişkin açıklamalar dikkate almalıdır.

5.6.1. Kimlik hırsızlığı

Kimlik dolandırıcılığı, bir kişinin başka bir kişinin isim, adres, doğum tarihi ve finansal hesap bilgileri gibi kimlik bilgilerini izinsiz olarak ve dolandırıcılık yapmak ya da başka suçları işlemek için kullanmasıdır.

Suçlunun mağdurun kimlik bilgilerini elde etmek için kullandığı yöntem genellikle bilinmez. Kişisel bilgileri elde etmenin yaygın yöntemleri arasında oltalama, veri ihlâlleri ve kötü amaçlı yazılımlar bulunmaktadır.

Kimlikler dolandırıcılık yapmak için farklı şekillerde kullanılmaktadır; bunların arasında mağdurların kişisel kimlik bilgilerini kullanarak izinsiz alışveriş

yapılması, banka hesabı açılması veya kredi çekilmesi ve tıbbi tedavi ve ilaç gibi hizmetler alınması yer almaktadır.

Kimlik hırsızlığı kendi başına bir suç teşkil etmediğinden, soruşturmaların, siber suçların bildirilmesine yönelik yasal çerçeveyi göz önünde bulundurması gerekecektir. Kimlik bilgilerinin suç işlemek için kullanıldığı durumlarda, cezai çerçeve genellikle, dolandırıcılığın veya başka bir suç eyleminin gerçekleştiğine dair delillere dayanmaktadır.

5.6.2. Hesap çalma

Hesap çalma, bir kimlik hırsızlığı biçimidir ve bir saldırganın, kullanıcının kullanıcı adı, parola veya PIN gibi hesap bilgilerine başarılı bir şekilde erişim sağlamasıdır. Saldırgan hesaba erişmek için bu kimlik bilgilerine ulaştığında, maddi kazanç sağlama amacıyla bilgi elde edebilir veya bir banka hesabından veya benzeri bir yerden izinsiz finansal işlemler gerçekleştirebilir.

Finansal hizmetlerin güvenlik sistemleri, hesap çalınması tehditlerine karşı kendilerini geliştirmiştir ve müşterilerin artık kanıtlayıcı bir kimlik doğrulama yöntemi (iki aşamalı kimlik doğrulama) kullanması beklenmektedir. Bu tür sistemler, müşterilerin doğrulama mesajlarını alabilecekleri cep telefonu, sosyal medya hesabı ve/veya e-posta hesabı bilgilerinin sağlanmasını gerektirir. Suçlular, çevrimiçi hesaplarda zafiyet yaratarak veya mağdurların cep telefonu numaralarından SIM kartlarını kopyalayarak bu ek güvenlik önlemlerini zayıflatmaya çalışırlar. Yetkililer bahse konu suç türlerini bildirirken bu yöntemleri göz önünde bulundurmalı ve raporlarında olası riskleri tanımlamalıdır.

5.6.3. Teknik destek dolandırıcılığı

Teknik destek dolandırıcılığı genellikle, saldırganın meşru bir teknik destek sağlayıcısı adına aradığını iddia ettiği ve rastgele arama yoluyla yapılan bir telefon görüşmesi aracılığıyla başlatılır. Saldırganlar genellikle Microsoft veya İnternet Hizmet Sağlayıcılarının teknik destek biriminden aradıklarını iddia eder ve mağduru, bilgisayarlarına veya cihazlarına uzaktan erişim sağlamaya ikna etmek için sosyal mühendislik becerilerini kullanmaya çalışırlar.

Uzaktan erişim sağlandıktan sonra, saldırgan kredi kartı numaraları ve benzeri kişisel bilgileri alabilir veya mağduru çevrimiçi hesaplarına girmeye ikna

ederek, oturumu açtığı sırada mağdurun bilgilerini gözlemleyip kaydedebilir.

Birçok teknik destek dolandırıcılığı, çağrı merkezi tipi bir kurgu kullanılarak gerçekleştirilir.

5.7. Web sitesi tahrifatı

Web sitesi tahrifatı, kötü niyetli kişilerin bir web sitesine erişim sağlayarak sitedeki içeriği başka mesajlarla değiştirdiği bir saldırı türüdür. Bu mesajlar, siyasi veya dini bir içerik, müstehcen bir dil veya web sitesi sahiplerini utandırabilecek başka uygunsuz bir içerik barındırabilir veya web sitesine belirli bir bilgisayar korsanı grubu tarafından erişildiğine dair bir bildirimi içerebilir.

Çoğu web sitesi ve web uygulaması, web sitesinde görüntülenen içeriği etkileyen veya şablonların ve sayfa içeriğinin nerede bulunduğunu belirten verileri, ortam veya yapılandırma dosyalarında depolar. Bu dosyalarda meydana gelen beklenmedik değişiklikler, güvenlik açığı yaşandığı anlamına gelebilir ve bir tahrifat saldırısına işaret edebilir.

Çoğu işletmenin bu tür saldırılarla başa çıkmak üzere hazırlanmış olay müdahale planları bulunur ve bu planlar kapsamında, tahrif edilmiş web sunucusunun daha detaylı araştırma amacıyla çevrimdışı bırakılması da yer alır. Bir sonraki adım, istismar edilen güvenlik açığının veya saldırı yönteminin belirlenmesidir. Söz konusu adım, SQL Enjeksiyonu saldırıları ve siteler arası komut dosyası saldırıları gibi, sık görülen istismar girişimlerinin araştırmasını da kapsamaktadır. Elektronik delillerin normalde bulunabileceği yerler arasında, verilerdeki değişikliklerin tarih ve saatlerini ve sunucuya bağlanan IP adreslerini gösteren sunucu kütükleri ve güvenlik duvarı kütükleri yer alır. Uzmanların soruşturma ve kütük analizi için kullanabileceği özel araçlar vardır.

Saldırganlar, saldırıya ait bazı detayları kendi web sitelerinde veya başka bazı kaynaklarda (Pastebin gibi) paylaşmış olabilir; bu yüzden açık kaynaklı istihbarat çalışması yürütülmesi bir diğer soruşturma yöntemi olarak düşünülebilir.

Cumhuriyet savcıları ve polis, saldırıya uğrayan web sitesinin müşteri iletişim planını da dikkate almalıdır; zira web sitesi müşterilerinin de saldırı hakkında ve saldırının web sitesindeki kaynaklara erişimi nasıl etkilediği konusunda bilgilendirilmesi gerekecektir.

5.8. Çevrimiçi çocuk istismarı ve sömürüsü

Çevrimiçi çocuk istismarı, çevrimiçi uşaklaştırmayı (grooming), canlı yayın açtırmayı, cinsel istismar materyallerinin kullanılmasını ve çocuklara cinsel amaçlarla şantaj yapılmasını içerir. Teknoloji ilerledikçe bu suçun yeni biçimleri ortaya çıkmakta ve çevrimiçi bağlantıya erişim arttıkça, daha fazla ülke ve bu ülkelerde yaşayan çocuklar istismardan etkilenmektedir.

Mevcut teknik erişim ve anonimliği korumaya yönelik araçlar, suçluların çocuklarla iletişim kurmasını, çocukların cinsel istismar içeren görüntü ve videolarına ulaşmasını ve bunları diğer suçlularla paylaşmasını hiç olmadığı kadar kolaylaştırmıştır. Suçluların görüntüleri paylaşmasının altında yatan motivasyon genellikle kâr elde etmek ve çocuklara karşı daha fazla cinsel istismarda bulunmaları için başkalarını teşvik etmektir.

Suçlular iletişim kurmak için darknet ve diğer anonim kanalları kullandığından, suçluların ve mağdurların tespit edilmesi genellikle çok zordur. Çocuk istismarı, suçlu ve mağdurun genellikle farklı ülkelerde bulunabilmesinden dolayı, birden çok uluslararası yargı sistemini ilgilendirmektedir. Örnekler arasında, çocukların canlı yayınlanan videolarda istismara uğradığı, cinsel işkence ve aşağılamanın uzaktaki bir suçlunun yönlendirmesiyle gerçekleştiği ve izleme başına ödeme yapılan cinsel istismarlar yer almaktadır. Durumu karmaşıklaştıran bir diğer unsur ise, çocukların akranlarıyla paylaşmak için kendi kendilerine ürettikleri ve suçluların eline geçen cinsel içerikli materyallerin giderek artmasıdır.

Soruşturmada, bahse konu suçların tecavüz ve ağır aşağılama da dâhil daha fazla cinsel istismara maruz kalmayı ve çocuk mağdurların yaşamlarına yönelik sürekli tehdit oluşturmayı da kapsadığı dikkate alınmalıdır. Bu, mağdurun tespit edilmesi, korunması ve güvenliğinin sağlanması için acil adımlar atılması gerektiği anlamına gelmektedir. Söz konusu suçlar, en ciddi suç türleridir ve kolluk kuvvetlerinin her türlü müdahalesi ivedilikle değerlendirilmelidir.

Birçok ülkede, çocuklara yönelik çevrimiçi suçların araştırılması için özel olarak görevlendirilmiş birimler bulunmaktadır. Bu suçlara yönelik tüm soruşturmalar iletişim verileriyle ilgili ciddi delil toplanmasına dayanır ve delil toplama süreci 7/24 Tek İrtibat Noktasının desteğiyle genişletilebilir. Birçok hizmet sağlayıcı, bu tür soruşturmaları aktif olarak desteklediğinden, söz konusu soruşturmalarda daha hızlı yanıt alınabilmektedir.

5.8.1. Cinsel amaçlı siber uşaklaştırma (grooming)

Cinsel amaçlı siber uşaklaştırma, bir kişinin, genç bir kişi veya çocukla çevrimiçi bir ilişki kurarak, söz konusu kişiyi cinsel bir eylemde bulunması için kandırması veya ona bu amaçla baskı yapmasıdır. Bahse konu eylem, kendi mahrem görüntülerini göndermesini, bir web kamerası önünde kendini teşhir etmesini ve/veya seks amacıyla buluşmayı içerebilir. Bu kılavuzun yazıldığı tarihte, siber uşaklaştırma Türkiye'deki yasal çerçeve kapsamında özel olarak düzenlenmiş bir suç değildir. Bununla birlikte, somut vakanın özelliklerine göre siber uşaklaştırma eylemleri TCK Madde 226'da düzenlenen "Müstehcenlik" suçu veya TCK Madde 105'te düzenlenen Cinsel Taciz veya TCK Madde 107'de düzenlenen şantaj gibi farklı suç tipleri bağlamında değerlendirilebilecek ve cezalandırılabilecektir. Ancak aşağıda belirtilen nedenlerle, mevcut suç tiplerine girmeyen eylemler de içermesi nedeniyle bu suçun özel bir suç olarak düzenlenmesinde hukuki yarar bulunduğu ileri sürülebilir. Nitekim birçok ülkede, cinsel amaçlı olan veya olmayan siber uşaklaştırma eylemleri giderek artan biçimde özel suç tipleri olarak düzenlenmektedir.

Siber uşaklaştırma vakalarında, yetişkin suçluların genellikle yaşları, ilgi alanları, cinsiyetleri ve iletişimin nedenleri konusunda yalan söyleyerek kimliklerine dair yanlış bilgiler verdiği görülmektedir. Suçlular, bilgi edinmek ve ilişkiyi başlatmak için mağdura birçok mesaj gönderebilmektedir. Suçlular, gizlilik ve mağdurun dış dünyayla (özellikle ebeveynleriyle ve bakıcılarıyla) iletişim kurmasını engellemek gibi yöntemler kullanarak mağdurda sahte bir emniyet ve güven duygusu yaratmaya çalışırlar.

Mesajlar masum bir şekilde başlayabilir, ancak suçlular iletişim sırasında giderek zorlayıcı hâle gelen cinsel sohbetler yapmaya başlayacaktır. Çocuklar genellikle deneyimsizlikleri, saflıkları ve kibarlıkları yüzünden bu iletişimi durduramamaktadır. Bazı durumlarda, çocuklar suçluya mahrem görüntülerini göndermekte ve kendilerini bir şantajın ortasında bulabilmektedir. Bu gibi durumlarda, suçlu daha mahrem ve daha açık cinsel görüntülerin gönderilmesini talep edebilmekte ve bu talebi daha önce çevrimiçi olarak elde ettiği görüntüleri ifşa etme tehdidiyle pekiştirebilmektedir.

Siber uşaklaştırma ihbarlarıyla ilgilenen polis ve cumhuriyet savcıları, olayın mağdur üzerindeki korku, hayal kırıklığı, öfke, utanç veya depresyon gibi etkilerini göz önünde bulundurmalıdır. Mağdurların özgüvenlerinin düştüğü ve kendilerine zarar vermeye veya intihara meyilli olabildikleri örneklerle de karşılaşılabilmektedir.

Soruşturmayı yürütenler, mağdurların normalde beklenenden çok farklı tepkiler verebileceğinin farkında olmalıdır. Bu tepkiler dikkate alınmalı ve mağdurun tepkileri raporlara geçirilmelidir. Soruşturmayı yürütenler, mağdurlara yöneltilen soru sayısını en aza indirmeli ve özellikle nedensel sorular sormaktan kaçınmalıdır (neden ... yaptın? veya ... yapmadın? gibi).

5.8.2. Siber zorbalık

Siber taciz ve çevrimiçi zorbalık olarak da bilinen siber zorbalık, çevrimiçi bir zorbalık ve/veya taciz türüdür. Bu tür davranışları tanımlamak için kullanılan diğer terimler arasında internet trollüğü ve siber takip sayılabilir. Bu tür suçlar, özellikle ergenlik çağındaki veya daha küçük yaştaki çocuklar olmak üzere, toplumun daha genç fertleri arasında giderek yaygınlaşmaktadır.

Bu suçlara delil teşkil edebilecek unsurlar arasında söylentiler yayan gönderiler paylaşmak, tehditlerde bulunmak, cinsel içerikli sözler söylemek, karşı tarafın rızası olmadan cinsel istismar materyallerini kullanmak, kişisel bilgileri ifşa etmek ve nefret söyleminde bulunmak yer alabilir. Bu zorbalık veya taciz eylemleri genellikle tekrarlanan eylemler olup mağdura zarar verme veya mağdurun zarar görmesini sağlama niyetiyle gerçekleştirilir.

Son yıllarda kadınlara yönelik siber şiddete vurgu yapan AİHM, Devletlerin ayrımcılık yapmama ilkesiyle ilgili yükümlülüklerinin altını çizmiştir:

"*Bu vesileyle Mahkeme son olarak, siber zorbalığın hâlihazırda kadınlara ve kız çocuklarına yönelik şiddetin bir yönü olarak kabul edildiğini ve siber mahremiyet ihlâlleri, mağdurun bilgisayarına izinsiz giriş ve özel veriler de dâhil olmak üzere veri ve görüntülerin ele geçirilmesi, paylaşılması ve manipüle edilmesi de dâhil çeşitli şekillerde ortaya çıkabileceğini belirtmiştir.*" (Buturaga - Romanya, 11 Şubat 2020, no: 56867/15, §74)

Söz konusu dava, başvuru sahibinin, tekrarlanan siber taciz eylemlerine karşı Rus makamlarının kendisini koruyamadığı iddiasıyla ilgilidir. Başvuru sahibi özellikle, eski partnerinin sahte sosyal medya profilleri oluşturmak için adını, kişisel bilgilerini ve mahrem fotoğraflarını kullandığını, el çantasına GPS izleyici yerleştirdiğini, sosyal medya aracılığıyla kendisine ölüm tehditleri gönderdiğini belirtmiş ve yetkililerin bu iddiaları etkin bir şekilde soruşturmadığını dile getirmiştir. (Volodina - Rusya (no. 2), 14 Eylül 2021, no: 40419/19)

Bu tür zorbalık ve tacizin mesajlarının iletilmesi, sadece mesajlaşma gibi tek bir yöntemle sınırlı olmayabilir ve anonim veya yarı anonim kanallarla gönderilebilecek metin mesajlarını, sosyal medya gönderilerini ve çevrimiçi forumlarda yapılan yorumları içerebilir.

Siber zorbalık ihbarlarıyla ilgilenen polis ve cumhuriyet savcıları, olayın mağdur üzerindeki korku, hayal kırıklığı, öfke, utanç veya depresyon gibi etkilerini göz önünde bulundurmalıdır. Mağdurların özgüvenlerinin düştüğü ve kendilerine zarar vermeye veya intihara meyilli olabildikleri örneklerle de karşılaşılabilmektedir.

İlk müdahaleyi yapan ekipler, mağdurların normalde beklenenden çok farklı tepkiler verebileceğinin farkında olmalıdır. Bu tepkiler dikkate alınmalı ve mağdurun tepkileri raporlara geçirilmelidir. İlk müdahaleyi yapanlar, mağdurlara yöneltilen soru sayısını en aza indirmeli ve özellikle nedensel sorular sormaktan kaçınmalıdır (neden ... yaptın? veya ... yapmadın? gibi).

5.8.3. Çevrimiçi cinsel cebir ve şantaj (Sextortion)

Çevrimiçi cinsel cebir ve şantaj, internet üzerinden gerçekleştirilen yeni bir suç olgusudur ve hem yetişkinleri hem de çocukları etkilemektedir. İnternetin yaygınlaşması ve kameralı ve video kayıt özellikli mobil cihazların internete bağlanabilmesi, bu suç türündeki artışın nedenlerinden bazılarıdır.

Çocukların hedef alındığı durumlarda, ana motivasyonlar arasında çocuklara yönelik cinsel ilgi ve/veya failin şantajdan mali fayda sağlamaya çalıştığı ekonomik menfaat elde etme motivasyonu yer almaktadır. Daha fazla bilgi için Europol web sitesinin cinsel cebir ve şantaj konulu raporu incelenebilir.[11]

Bu tür cinsel cebir ve şantaj suçlarının altında yatan daha karmaşık motivasyonlar da olabilmektedir. Örneğin, ergenlik çağındaki gençler gibi birçok genç, kendi ürettikleri cinsel içerikli materyalleri (KÜCİM) alarak bunları flört ve/veya deneyim biçimi olarak başkalarıyla paylaşabilmektedir. Diğer motivasyonlar arasında kötü niyet veya dikkat çekme, popülerlik ve onaylanma isteği gibi bir tür sosyal kazanım elde etme isteği bulunmaktadır. 18 yaşın altındaki çocuklar ve gençler, 18 yaşın altındaki bireylerin cinsel istismar materyallerini oluşturma ve dağıtma gibi davranışları sistemli olarak suç sayan yasal çerçeveden genellikle habersizdirler.

11 https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

KÜCİM oluşturan ve paylaşan ergenlik çağındaki kişiler ve gençler, bunu kendi rızalarıyla yaptıkları gibi, cebren de yapabilmektedir. Bahse konu cebir soruşturma ekibi tarafından dikkate alınmalı ve öncelikle özel olarak uzmanlaşmış birimlerin veya uzmanların desteği aranmalıdır. Bu tür örnekler arasında yer alabilecek durumlar aşağıdaki gibidir:

- KÜCİM'in başka bir kişinin talebi üzerine oluşturulması
- Reşit olmayan birine, talep etmediği bir resmin gönderilmesi
- Daha önce KÜCİM oluşturmuş diğer çocuk ve gençlerin yeni materyaller yollamaları için tehdit edilmesi ve cebre maruz kalması
- Bu tür materyallerin başka kişilere ve tekrar tekrar dağıtılması.

Gençler arasında KÜCİM paylaşımı, özellikle bir arkadaş veya akran grubu içinde bu gençlerin kendi rızası ile gerçekleştiğinde, karmaşık bir senaryo ortaya çıkmaktadır. Görüntülerin özneleri bunu normal bir davranış olarak tanımlayabilmekte ve kendilerini "mağdur" olarak görmeyebilmektedir.

Risk azaltma tedbirleri, çocukların ve gençlerin çevrimiçi iletişim sırasında kabul edilebilir ve kabul edilemez davranışları tanımlayabilmelerine ve ayırt etmelerine olanak tanıyan eğitim ve farkındalık faaliyetlerini kapsayabilir.

5.8.4. Çocuğun (Cinsel) İstismarı Materyali

Uluslararası siber suç birimlerinin ve dijital cihazların dâhil olduğu adli tıp soruşturmalarında en çok bildirilen ve karşılaşılan suç alanlarından biri, çocuğun (cinsel) istismarı materyallerinin (ÇCİM) bulundurulması, sergilenmesi, üretilmesi ve dağıtılmasıdır.

ÇCİM, 18 yaşın altındaki bir kişinin resimleri ve video materyalleri de dâhil olmak üzere, aşağıdaki durumlarda olan bir çocuğa ait cinsel bir görüntüyü içerir:

- Çıplak veya kısmen giyinik
- Cinsel poz verir şekilde
- KÜCİM
- Penetratif ve penetratif olmayan cinsel aktivitede bulunmakta olan

Hareketsiz görüntüleri, video kayıtlarını ve sözde fotoğrafları içerebilecek görüntülerin depolandığı mecralar yasal çerçeveyle tanımlanmıştır.

Yasal çerçeve, çocukların görüntülerinin bulundurulması, alınması, oluşturulması ve dağıtılmasını içeren suçları belirlemiştir (TCK 226).

- Bulundurma – basılı kopya veya dijital kopya olsun, kişinin elinde bir ÇCİM olması anlamına gelir.
- Dağıtma – sohbet odaları, e-posta, mesaj, telefon uygulamaları, dijital bellek depolama cihazları ve dosya paylaşım web siteleri aracılığıyla bir ÇCİM'nin başka bir kişiye gönderilmesi anlamına gelir.
- Üretme – bir ÇCİM'nin oluşturulması, örneğin elektronik kopyasının yapılması anlamına gelir ve kullanıcının, bir kopyayı (dosya paylaşım web sitelerinden otomatik olarak indirilen görüntüler dâhil) kasıtlı olarak bir cihaza veya bilgisayara kaydetmesi de üretmeye dâhildir.

Birçok uluslararası kuruluş (Interpol ve Europol gibi), farklı uygulamalar, sohbet odaları ve dosya paylaşım ağları üzerinden çevrimiçi ÇCİM paylaşan suçluları izleyen takip yazılımları kullanmaktadır. IP adresini, çevrimiçi faaliyetin ilgili zamanlarını ve şüphelinin kimliğini belirleyebilecek diğer bilgiler gibi istihbarat bilgileri Türkiye'deki kolluk kuvvetleriyle paylaşılabilir.

Genel olarak, bu kuruluşlar, kolluk kuvvetlerinin ve cumhuriyet savcılarının ceza soruşturması başlatmasına olanak tanıyan yeterli istihbarat paylaşımı yapmaktadır. Bu gibi durumlarda normal protokol, bir arama emri çıkartılması ve şüphelilerin binasında bulunan ve ÇCİM de dâhil elektronik delil içerebilecek dijital cihazlara elkoyulmasıdır. Bu soruşturmalar, büyük ölçüde söz konusu lokasyonda ele geçirilen delillere dayanır. Bu yüzden söz konusu çevrimiçi takip araçlarının Türkiye ve başka ülkelerdeki diğer soruşturmalarda kullanılabilmesini riske atmamak için, soruşturmalar bu araçların korunmasını amaçlamalıdır.

5.8.5. İnternet üzerinden hakaret ve aşağılama

Bu suçlar (TCK 125 (Hakaret Suçu) ve TCK 299 (Cumhurbaşkanına Hakaret Suçu))[12] Türk Ceza Kanunu'nda ayrıntılı bir şekilde düzenlenmiştir. Bu tür soruşturmalardaki normal adımlardan biri, uluslararası kurumlardan (kolluk kuvvetleri, yargı makamları, internet hizmet sağlayıcıları, sosyal medya ve çok

12 Buna ilave olarak AİHM, "Cumhurbaşkanına hakaret" suçunun varlığının bile, demokratik bir toplumda ulaşılmak istenen ve gerekli görülen meşru amaçlarla orantılı olmaması nedeniyle 10. Maddenin (ifade özgürlüğü) ihlâli olduğuna karar vermiştir (Vedat Şorli - Türkiye, 19 Ekim 2021, no: 42048/19)

uluslu hizmet sağlayıcılar) talepte bulunmaktır. Avrupa ve Kuzey Amerika'daki çoğu ülke bu konuları Özel Hukuk kapsamında ele almakta ve ceza mahkemeleri, cumhuriyet savcıları ve polis süreçlere dâhil olmamaktadır.

Bu nedenle, bu ülkelere veri ve iletişim bilgilerini elde etmek amacıyla iletilecek talepler, mütekabiliyet olmadığı için sonuçsuz kalacaktır. Bu ülkelerdeki yasal çerçeve, internet üzerinden hakaret ve aşağılama vakalarında veri ve iletişim bilgilerinin kolluk kuvvetleri veya yargı makamları ile paylaşılmasına izin vermemektedir.

Birçok Avrupa ülkesi, bu soruşturmaların ve müteakip mahkûmiyet kararlarının çoğunun AİHS Madde 10 – İfade Özgürlüğü kapsamında ihlâl riski taşıdığı görüşünü benimsemekte ve bu sebeple, internet üzerinden hakaret ve aşağılamayı suç sayan yasal bir çerçeve oluşturmamaktadır.

6. Raporlama aşamasında ilk yapılacaklar

6.1. İlk adımlar

Bu bölümde, siber suçlarla ilgili soruşturmalar söz konusu olduğunda ilk aşamalarda üstlenilmesi gereken iki temel görev açıklanmaktadır: Bu görevlerden ilki elektronik delillerin tespit edilmesi ve bunlara elkoyulması; ikincisi ise siber suç mağdurlarının şikâyetlerinin alınması ve soruşturmanın ilk adımlarının atılmasıdır.

Daha ayrıntılı bilgi, raporlamayı yapacak memurların siber suç ihbarı aldığında atması gereken adımları detaylı bir şekilde anlatan "Avrupa Konseyi Siber Suç Soruşturmalarına İlk Müdahaleyi Yapanlara Yönelik Kılavuz YENİ" (2021) belgesinde bulunabilir.

Siber suç ihbarını alarak ilk müdahaleyi yapan kişi veya cumhuriyet savcısı tarafından atılacak ilk adımlar, genellikle şikâyetin açıklanması amacıyla aşağıdaki hususları içerir:

- Mağdurun şikâyet dilekçesini doldurmasına yardımcı olunması ve destekleyici delillerin alınması
- Şikâyetin biçimi ve yürürlükteki ceza kanunlarının niteliği
- Gerekli bilgilerin ve olaya yönelik açıklamaların alınması
- Mağdur veya tanığın elinde olmamaları hâlinde, destekleyici delillerin yerinin tespit edilmesi

Dijital cihazların tespit edilmesi ve elektronik delillerin elde edilmesinde, ilk müdahaleyi yapan kişi veya cumhuriyet savcısı elektronik delilleri diğer delil türlerine benzer şekilde değerlendirmeli, böylelikle delillerin kabul edilebilirliği, bütünlüğü ve doğruluğu sağlanmalıdır. Delil zinciri, elektronik delillerin ele alınmasını ifade eder ve yetkililer, soruşturma ve müteakip mahkeme işlemleri boyunca sanığın âdil yargılanması ve uygun adalet dengesinin korunması için

kurumsal usûllere uygun davranmalıdır. Bu adımlar, elektronik delillere ait tüm hareketlerin ve bu delillerin yetkililer ve/veya birimler arasında aktarımının belgelendirilmesini içerir. Kaydedilmesi gereken detaylar arasında, kişilerin adları, konumlar, tarihler, saatler ve delil işlenmesine ilişkin tüm koşullar yer alır. Daha detaylı bilgi, akış şemaları ve belge örneği formları için, "Elektronik Delil Kılavuzuna" bakınız.[13]

İlk ihbar sırasında veya soruşturma aşamasında elektronik delilleri toplayan polis memurları, cihazın açık mı yoksa kapalı mı olduğuna dikkat etmeli ve bunu kaydetmelidir. Şayet cihaz açıksa, özel bir özen gösterilmeli ve bu konuda eğitim almış bir memurdan, siber suçlar biriminden veya adli bilişim biriminden tavsiye alınmalıdır. Cihaz kapalıysa, AÇILMAMALIDIR. Polis memuru, cihazdaki herhangi bir hasar gibi her türlü durumu kaydetmeli ve elektronik delillerle veya dijital cihazla tüm etkileşimlerini belgelemelidir.

Elektronik deliller üzerinde çalışırken, çevrimiçi verilerin yerlerinin tespit edilmesi, korunması ve elde edilmesinde zamanlama genellikle kritiktir ve/veya fırsatlar sınırlıdır. Bunun nedeni, normal sistem süreçlerinin bir parçası olarak meydana gelen veri değişiklikleri olabildiği gibi, şüphelinin o esnada veya daha sonra uzaktan bağlantı yoluyla delilleri gizlemeye çalışabilecek olmasıdır. Polis memurunun ve/veya cumhuriyet savcısının, bu sorumlulukları nasıl olsa daha sonra soruşturmayı yürüten başka biri yerine getirir diye düşünmemesi veya siber suçun çözülemeyeceğini varsaymaması ve tüm materyalleri toplaması önemlidir.

Soruşturmayı yürüten kişiler, delil ve bilgi talebinde bulunurken, verilerin genellikle suça veya soruşturmaya dâhil olmayan kişilere ait kişisel bilgiler de içerdiğini göz önünde bulundurmalıdır. Bu durum genellikle ikincil müdahale olarak adlandırılır. İkincil müdahale, tanık ve şüphelilerin ortaklarını ve aile üyelerini de kapsayabilir. Soruşturmayı yürüten memurlar ve cumhuriyet savcıları, AİHS'nin 8. maddesinde (Özel Hayata ve Aile Hayatına Saygı Hakkı) tanımlanan güvenceler açısından gerekli olduğu gösterilmedikçe, suça dâhil olmayan kişilerin özel hayatına müdahalenin mümkün olduğunca en aza indirilmesi gerektiğini her zaman göz önünde bulundurmalıdır.

13 "Elektronik Delil Kılavuzu - POLİS MEMURLARI, SAVCILAR VE HÂKİMLER İÇİN TEMEL BİR REHBER", Sürüm 2.1, 03/2020, Avrupa Konseyi, https://www.coe.int/en/web/octopus/training

Ayrıca, hâlihazırda adli işlemlerde ve kolluk faaliyetlerinde kişisel verilerin işlenmesine yönelik özel bir düzenleme bulunmamakla birlikte, Anayasa Mahkemesi kararlarında, buna ilişkin özel bir kanun olmasa bile yargı makamlarının, anayasada yer alan temel haklar çerçevesinde gerekli değerlendirmeleri yapması gerektiği belirtilmektedir (E.Ü., AYM GK, 17 Eylül 2020, No: 2016/13010). Bu nedenle, Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde öngörülen kişisel verilerin işlenmesine ilişkin genel ilkeler tüm yargılama süreçlerinde dikkate alınmalıdır:

"MADDE 4 – (1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usûl ve esaslara uygun olarak işlenebilir.
(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:
a) Hukuka ve dürüstlük kurallarına uygun olma.
b) Doğru ve gerektiğinde güncel olma.
c) Belirli, açık ve meşru amaçlar için işlenme.
ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

6.2. Aciliyetin değerlendirilmesi, zararın azaltılması

Kişilere, işletmelere ve kurumlara yönelik devam eden saldırıların genellikle maliyetli olduğunun veya ciddi riskler taşıdığının bilinmesi önemlidir. İlk müdahaleyi yapan kişinin veya cumhuriyet savcısının olay yerini koruması önemli olsa da BİT ağlarının daha fazla riske ve potansiyel zarara maruz bırakılmamasına, daha fazla mali kaybın yaşanmamasına ve mağdurun zarar görmemesine dikkat edilmesi önemlidir.

Birçok işletme ve kurumun, kötü amaçlı yazılım bulaşması, BİT sistemlerine izinsiz erişim ve hizmet engelleme saldırıları gibi siber güvenlik olaylarıyla başa çıkmak için özel prosedürleri bulunur. Genellikle bu ilk adımlar delillerin korunmasıyla ilgili olmayıp herhangi bir saldırının etkisini azaltmak için bulaşmanın kontrol altına alınması ve hafifletilmesine yönelik önlemlere odaklanır. Bu süreçler, BİT sistemlerinde depolanan verileri değiştirmekte ve elektronik delillerin kullanılabilirliğini etkilemektedir. Alternatif olarak, olayın izlenmesine ve saldırgan ve saldırıda kullandığı yöntem hakkında delil olarak kullanılabilecek bilgilerin toplanmasına odaklanılabilir.

6.3. Elektronik delillerin korunması için acil önlemlerin alınması

Elektronik delillerin işlenmesi; delilin tespit edilmesi, toplanması, elde edilmesi, incelenmesi ve raporlanması olarak adlandırılan beş adımdan oluşmaktadır. Bu adımların bazıları ilk müdahaleyi yapan kişinin sorumluluğu dışında olsa da veri toplamanın en önemli kısmını, delilin tespit edilmesi ve toplanması adımlarını içeren "delillerin korunması" oluşturmaktadır. Daha ayrıntılı bilgi için bu kılavuzun 9.3 ve 9.4 bölümlerine bakınız.

Sunucularda ve genellikle Türkiye dışındaki Çok Uluslu Hizmet Sağlayıcılarda saklanan elektronik deliller olabileceği unutulmamalıdır. E-posta sunucuları, sosyal medya hesapları ve bulut depolama çözümleri bu örnekler arasında sayılabilir. Delil niteliğindeki bu tür verilerin korunması için, onaylanmış kanallar aracılığıyla, uygun yasal çerçeve kullanılarak ve genellikle bu verileri depolayan kurumla iş birliği içinde somut adımlar atılmalıdır.

Türkiye'deki onaylanmış kanallar arasında, Emniyet Genel Müdürlüğü bünyesinde haftanın yedi günü ve günün 24 saati hizmet veren özel bir Tek İrtibat Noktası (7/24 TİN) bulunmaktadır.

7/24 Tek İrtibat Noktası ve ulusal siber suçlar birimi, ilk müdahaleyi yapan kolluk kuvvetlerine destek ve tavsiye veren sürekli bir referans noktası olarak hizmet vermektedir. Olay raporunu hazırlayan memurun ve cumhuriyet savcısının, gerektiğinde, daha karmaşık siber suç vakalarında ve elektronik delillerle ilgili konularda rehberlik talebinde bulunmayı değerlendirmesi önemlidir.

7. IP adresleri ve diğer tanımlayıcılar

7.1. IP adresleri – genel

İki veya daha fazla bilgisayar (veya ağa bağlı dijital cihaz) veri kabloları veya kablosuz bağlantıyla birbirine bağlandığında bir "ağ" kurulmuş olur. Bir ağdaki bu tür cihazlar, verileri ve diğer kaynakları paylaşabilir ve genellikle kapsamlarını genişleten ve mevcut işlevlerini artıran ek donanım bileşenlerine bağlanırlar. Bilgisayar ağları, evlerde bulunan ağlar gibi sınırlı olabileceği gibi (örneğin, bir internet modemini paylaşan aile üyelerinin kurduğu ağlar) büyük şirketler veya hükümetler tarafından kullanılan ve yüzlerce, hatta binlerce bilgisayarı birbirine bağlayan ağlar gibi kapsamlı da olabilir. Bu ağlar, Yerel Alan Ağları olarak tanımlanmaktadır ("özel ağ" veya "dâhili ağ" tabirleri de kullanılmaktadır). Bilgisayarlar ve dijital cihazlar Geniş Alan Ağına da (internet gibi) bağlanabilir.

Ağlardaki diğer cihazlarla iletişim kurmak için, farklı türde adresleme protokolleri kullanılır. Bunların arasında İnternet Protokolü (IP), Bağlantı Noktaları, Ortam Erişim Kontrolü ve İletim Kontrol Protokolleri (TCP) yer almaktadır. Çoğu soruşturmada, sorunları çözmek ve saldırganların ve ilgili cihazların kimliğini belirlemek için IP adreslerinden yararlanılır. Bu ve diğer adresleme protokollerinin tüm ayrıntılarının anlaşılması için daha fazla araştırma yapılması gerekmektedir.

İnternette, IP adreslerinin çoğu yönlendiricilere (router) atanır. Bir yönlendiricinin rolü, veri paketlerini almak ve bir konumdan diğerine göndermek ve iletmektir. Kaynak IP adresinden hedef IP adresine gönderilen bir veri paketi normalde birkaç farklı yönlendirici üzerinden geçecektir. Soruşturmada, dosya her zaman kaynak ve hedef IP adreslerini dayanak alacaktır (ara yönlendirici adreslerini değil).

Kolluk kuvvetlerinin yürütmesi muhtemel soruşturmaların çoğunda, bir suçluyla ilişkilendirilebilecek bir yönlendiricinin IP adresinin tespit edilmesine veya delillerin fiziksel yerinin belirlenmesine çalışılır. Bir evde, işyerinde veya

başka türlü bir kurumda bulunan özel bir ağın sınırları içinde, bir İnternet Hizmet Sağlayıcısı (İHS) tarafından kendisine atanan genel bir IP adresine sahip bir yönlendirici bulunur. İnternet Hizmet Sağlayıcısı, IP adreslerini kime atadığının (kiraladığının) kaydını saniye saniye tutacaktır. İnternet Hizmet Sağlayıcısı bu gibi durumlarda, soruşturmayı ilgilendiren bir IP adresine sahip olan kişilerin müşteri bilgilerini tüm detaylarıyla sağlayabilir.

IP adresleri her zaman kalıcı olarak atanmadığından (kiralanmadığından), bir cihazın adresinin zaman zaman değişmesi muhtemeldir (Dinamik IP adresi). Bu nedenle, bir IP adresini çözmeye çalışırken, tarih-saat damgasının ve saat diliminin tam olarak belirlenmesi ve bu bilgilerin IP adresi atamasını çözmek amacıyla yapılan tüm taleplere eklenmesi gerekir.

7.2. Yönlendiriciler ve özel IP adresleri

Kendisine genel bir IP adresi atanan bir yönlendirici, her zaman için 'özel bir ağın sınırları içinde' bulunur, ancak bu tek başına, özel ağ içinde yer alan ve soruşturmaya konu teşkil eden herhangi bir faaliyetten sorumlu olabilecek cihazı tanımlamak için yeterli bilgi sağlamaz. Yönlendirici, genel bir IP adresinin (İnternet Hizmet Sağlayıcısı tarafından verilen) yanı sıra, farklı bir IP adresi kümesinin bulunduğu özel ağa açılan bir ağ geçidi görevi görür. Ağ içindeki bu IP adresleri, yönlendirici tarafından verilen özel IP adresleridir.

Bu ağ geçidi yönlendiricileri (aksi istenmediği takdirde), özel ağa bağlanan, kablolu veya kablosuz dâhili aygıtların ve atanan özel IP adreslerinin kaydını tutar.

(Varsayılan ağ geçidi görevi gören) yönlendiricinin kütük dosyalarının incelenmesi, olay sırasında bağlanan cihazı veya soruşturmayı ilgilendiren suçu tanımlayabilir. Bu, özellikle işletmeler veya benzer büyük özel ağlarda geçerlidir ve yönlendiriciye bağlanan tüm bilgisayarların analizini engelleyebilir.

Yönlendiricilerin incelenmesi, uzman adli bilişim memurları veya bu konuda eğitim almış ilk müdahale ekipleri tarafından yapılmalıdır.

7.3. IP adresleri – cep telefonlarına atama

Bir cep telefonunun veya mobil cihazın IP adresinin, iletişim kurduğu sunucu açısından her zaman benzersiz ve kalıcı olduğuna dair yaygın bir yanlış kanı vardır. Ancak durum böyle değildir.

Mobil cihazlar bir Wi-Fi ağı üzerinden talepte bulunabilir ve Wi-Fi yönlendiricinin IP adresini devralabilir. Bu, aynı Wi-Fi ağındaki tüm kullanıcıların aynı özel ağın bir parçası olacağı ve aynı genel IP adresine sahip olacağı anlamına gelmektedir.

Bu durum, hücresel ağlarda da benzer şekilde gerçekleşir. Kullanıcılar aynı hücresel ağı kullanan benzer coğrafi konumlarda olduğunda, cihazlar en yakın hücresel yönlendiricinin IP adresini devralacaktır.

Hücresel cihazların sayısı nedeniyle, soruşturmayı yürüten kişinin veya cumhuriyet savcısının, doğru IP adresini ve tam tarih ve saat ile birlikte iletişimde kullanılan bağlantı noktası (port) numarasını sağlayabilmesi çok önemlidir. Bağlantı noktası numarası, cihazın ilgili zamanda bağlı olduğu sunucudan elde edilebilir.

Abone bilgilerinin alınmasına yönelik talepleri destekleyebilmek adına, tüm bu bilgilerin iletişim hizmet sağlayıcısına sunulması gerekecektir.

Daha ayrıntılı bilgi, Emniyet Genel Müdürlüğü bünyesindeki 7/24 Tek İrtibat Noktasından alınabilir.

7.4. Sanal Özel Ağ (VPN) ve Onion Router (TOR) - Dark Web

VPN, şifreleme kullanarak internete bağlanmanızı sağlar. Şifreleme, (kablosuz ağlar gibi) tespit edilebilecek ağlar üzerinden gerçekleşen iletişime güvenlik ve gizlilik ekler.

VPN, kullanıcıların bir VPN hizmet sağlayıcısı tarafından işletilen uzak bir sunucuya verilerin gönderildiği şifreli bir tünel oluşturmasına olanak tanır. VPN sunucusu daha sonra verileri, kullanıcının bağlanmak istediği siteye, şifrelenmiş ve bilgisayar korsanlarının ve diğer siber suçluların meraklı gözlerinden gizlenmiş, güvenli bir şekilde gönderir. Site yalnızca VPN servis sağlayıcısının IP adresini kaydedecek ve bu nedenle kullanıcının IP adresini sunucudan gizleyecektir.

Yasal olarak faaliyet gösteren VPN hizmet sağlayıcıları bazı kütük verilerini saklarken, birçok VPN hizmet sağlayıcısı bu bilgileri saklamamaktadır. Bazı VPN hizmet sağlayıcıları ise kolluk kuvvetleriyle etkileşime girmeyecek veya yasal taleplere yanıt vermeyecektir.

TOR, anonim iletişimi sağlamak için kullanılan ücretsiz açık kaynaklı bir yazılımdır. İnternet trafiğini yedi binden fazla aktarıcıdan oluşan ücretsiz, dünya çapında, gönüllü bir yer paylaşımı ağı üzerinden yönlendirerek kullanıcının

konumunu ve kullanımını çevrimiçi takip faaliyeti yürüten ve trafik analizi yapan herkesten gizler. TOR kullanımı, bir kullanıcının internet etkinliğinin izlenmesini daha zor hâle getirir.

TOR'un kullanım amacı, kullanıcılarının kişisel gizliliğinin yanı sıra, TOR çıkış düğümlerini kullanarak IP adresi anonimliği yoluyla gizli bir şekilde iletişim kurma özgürlüklerinin ve kâbiliyetlerinin de korunmasıdır.

TOR ve VPN'ler bazı açılardan benzer şekilde çalışmaktadır. Ancak her ikisi de kolluk kuvvetlerinin şüphelilerin yerini tespit etmesini zorlaştırmakta ve TOR, TOR ağını kullanarak gizli hizmetlerin (darknet sitelerinin) konumunun açığa çıkmasını engellemektedir.

Dark Web (Karanlık Ağ), internetle aynı fiziksel ağı kullansa da farklı bir dâhili ağ ve adres alanı kullanmaktadır. Soruşturmayı yürüten kişinin web sitesinin içeriğini görmek için Dark Web'in URL'sini (Alan Adını) bilmesi ve ayrıca Dark Web'in dâhili ağı üzerinden bağlanması gerekecektir.

Bir soruşturmanın VPN ve TOR kullanımıyla ilgili olması durumunda, Emniyet Genel Müdürlüğünün veya Jandarmanın Siber Suç Birimlerinden destek ve tavsiye alınması önerilir. "Dark Web", TOR üzerinde bulunan suç amaçlı web siteleri için konuşma dilinde kullanılan tabirdir. Dark Web üzerinde, standart arama motorları kullanılarak arama yapılamamaktadır.

Dark Web'e ilişkin soruşturmalar, bu kılavuz belgesinin kapsamının ötesine geçen, uzmanlık gerektiren bir görevdir. Ancak, aşağıdaki okuma listesi okuyucuları doğru noktalara yönlendirebilir:

- Dark Web'i keşfetmek için yeni başlayanlara yönelik bir rehber: https://turbofuture.com/internet/A-Beginners-Guide-to-Exploring-the-Darknet
- Deep Web (Derin İnternet) Bağlantıları: https://deepweblinks.org
- Deep Web Dizinleri ve arama motorları: http://www.thehiddenwiki.net/deep-web-directories-search-engines/
- TOR hizmetleri ve TOR ağının unsurlarına yönelik rehber: https://en.wikibooks.org/wiki/Guide_to_Tor_hidden_services_and_elements_of_the_Tor_network
- Dark Web Soruşturmaları- Adli Bilişim Uzmanları için Çevrimiçi Anonimliğin Zorlukları, https://articles.forensicfocus.com/2014/07/28/investigating-the-dark-web-the- challenges-of-online-anonymity-for-digital-forensics-examiners/

8. Kripto para birimlerini de içeren sanal ödeme sistemleri

8.1. Sanal para birimleri

Sanal para birimi şu şekilde tanımlanabilir:

- Bir değişim aracının
- ve/veya bir hesap biriminin
- ve/veya bir tasarruf aracının dijital sureti
- sanal para birimi yukarıdaki işlevleri, sanal para biriminin kullanıcı topluluğu içinde anlaşma sağlayarak yerine getirir.

8.2. Kripto para birimleri

Mali Eylem Görev Gücü (FATF), **Kripto Para Birimini** şu şekilde tanımlamıştır:

- matematik tabanlı bir para birimidir
- merkeziyetiz, dönüştürülebilir bir sanal para birimidir
- kriptografi ile korunur
- değerin bir kişiden (birey veya kurum) diğerine transfer edilmesi için, genel ve özel anahtarlar kullanılır
- ve her transfer edildiğinde kriptografik olarak imzalanmak zorundadır.

Avrupa Konseyi, kripto para birimleri, bunlara ilişkin kavramlar ve bu para birimlerine nasıl elkoyulacağı hakkında derinlemesine bilgi sunan bir "Kripto Para Birimlerine Elkoyulması Kılavuzu" yayınlamıştır[14]. Kripto para madenciliği, blokzinciri (blockchain) ve analiz araçları gibi konularla ilgili ayrıntı ve bilgi düzeyi, bu belgenin kapsamı dışındadır.

Bir kimsenin (şüpheliler de dâhil) kripto para birimine sahip olmasının iki ana yolu vardır. Bunlardan ilki, bilgisayarına yazılım indirmek veya bir kripto para adresinin veya cüzdanın (sanal cüzdan) özel anahtarını muhafaza eden

14 https://www.coe.int/en/web/octopus/home?desktop=true#{%2264860390%22:[1]}

bir cihaza sahip olmaktır. Diğer yol ise, bu hizmetin bir Sanal Varlık Hizmet Sağlayıcısından (Coinbase, Binance, Kracken, vb.) alınması ve bu kuruluş bünyesinde bir hesabınızın olmasıdır.

Arama ve elkoyma işlemleri sırasında, kolluk kuvvetlerinin kripto para birimlerine elkoyabileceğinin bilinmesi önemlidir. Bu, suç geliri olan paraya ve diğer varlıklara elkoyulması gibi görülmelidir. Bununla birlikte, kripto para birimlerini depolayan sanal cüzdanlara erişim genellikle korunur. Bir bilgisayar sisteminde depolanan olası kimlik bilgilerinin yanı sıra, başka parolalara, kurtarma cümlelerine (seed phrase) veya iki aşamalı kimlik doğrulama cihazlarına ihtiyaç duyulabilir. Bu nedenle, soruşturmayı yürütenler arama mahallindeki cihazlara ve izlere bakmalıdır.

Kripto para birimlerine elkoyulması ve bunların müsaderesi için tüm işlemlerin ivedilikle gerçekleştirilmesi zorunludur. Bunun nedeni, sanal cüzdanların kopyalanabilmesidir. Bu özellik, suçluların, varlıkları çok hızlı bir şekilde elkoyma sürecinin ulaşamayacağı bir yere taşımasına olanak tanımaktadır. Elkoyulan fonlar bir Devlet Cüzdanına yerleştirilmeli ve bu cüzdana erişim sıkı bir şekilde kontrol edilmelidir. Fonların uygun bir zamanda yasal para birimlerine dönüştürülmesini yönetmek için ilave operasyonel süreçler ve/veya kararlar gereklidir. Daha detaylı bilgiye, yukarıda ayrıntıları verilen yayınlanmış kılavuzdan ulaşabilirsiniz.

Sanal Varlık Hizmet Sağlayıcıları tarafından tutulan fonlar için, bir kolluk görevlisi veya cumhuriyet savcısı, bu kurumlardaki özel irtibat kişileri aracılığıyla doğrudan ve ivedilikle bu hizmet sağlayıcılarla iletişime geçmelidir. Fonlara elkoyulmasıyla ilgili talep, Türkiye'de elkoyma ve müsadere süreçlerini kolaylaştırmak amacıyla gerekli yasal belgeler eşliğinde yapılmalıdır.

9. Arama ve Elkoyma – Elektronik Deliller

Elektronik delillerin aranması ve bunlara elkoyulması, birçok soruşturmada oldukça önemli bir adımdır. Bu kılavuzda, elektronik delillerin kasıtlı veya kasıt dışı olarak silinmesinin, değiştirilmesinin veya üzerine başka veri kaydedilmesinin kolay olduğu açıklanmıştır.

Soruşturma kapsamında elektronik delillerin yeri tespit edildiğinde, delilin orijinal haliyle muhafaza edilmesine yönelik tüm adımlar polis ve/veya cumhuriyet savcısı tarafından atılmalıdır. Birçok durumda, 7/24 Tek İrtibat Noktasını kullanılarak gayri resmi bir talepte bulunmak yeterli olacaktır. Polis ve/veya cumhuriyet savcısı, güvenilir iletişim yöntemleri aracılığıyla hizmet sağlayıcıyla iletişime geçerek söz konusu verilerin korunmasını talep edecektir. Sonrasında, arama emirleri ve üretim emirleri gibi yasal çerçeveler kullanılarak, koruma altına alınan bu verilerin delil niteliği taşıyacak şekilde cumhuriyet savcısına sunulması talep edilmelidir. Örnek olarak e-posta hesapları, sosyal medya hesapları, iletişim verileri ve bulut kaynaklarında depolanan veriler verilebilir.

Verilerin muhafaza edilmesi talebinde bulunulmaması, anlamlı delillerin kaybedilmesine neden olabilir. Bu süreç, elektronik delillere elkoyulmasını amaçlayan günümüz soruşturmalarının önemli bir bileşenidir.

Elektronik delillerin aranması ve bunlara elkoyulmasına yönelik tüm işlemler, âdil yargılanma hakkı (Madde 6), özel hayata ve aile hayatına saygı hakkı (Madde 8)[15][16] ve ifade özgürlüğü (Madde 10)[17] gibi temel haklara müdahale açısından değerlendirilmelidir. Elektronik delillerin kabul edilebilirliğine ilişkin değerlendirmeler, haklara ilişkin denge testini ve delillerin mahkûmiyet üzerindeki etkisini de içermelidir[18]. Bunlara ek olarak, gerekli usûli güvencelerin uygulanması ve bunlara saygı gösterilmesi gerekmektedir.

9.1. Üretim emirleri

Üretim emirleri de siber suçlarla mücadelede elektronik delil toplanmasına yönelik değerli bir kaynak sunmaktadır. Siber suçlarda neredeyse her türlü teknoloji kullanıldığından, bir ceza soruşturmasında ilgili olabilecek üç tür veri; yani abone bilgileri, trafik verileri ve içerik verileri, bu verileri elinde bulunduran farklı hizmet sağlayıcılardan (telekom operatörleri, internet hizmet sağlayıcıları,

15 AİHM, iletişimin denetlenmesini düzenleyen Rusya'daki mevzuat hükümlerinin, keyfiliğe ve herhangi bir gizli takip sisteminin doğasında bulunan ve özellikle Rusya gibi, gizli servislerin ve polisin teknik yollarla tüm cep telefonu iletişimlerine doğrudan erişebildiği bir sistemde özellikle yüksek olan kötüye kullanım riskine karşı yeterli ve etkili güvenceler sağlamadığını tespit ederek, Sözleşme'nin 8. maddesinin (özel hayata ve haberleşmeye saygı hakkı) ihlâl edildiğine karar vermiştir. (Roman Zaharov - Rusya, 4 Aralık 2015)

16 AİHM, Sözleşme'nin 8. maddesinin (haberleşmeye saygı hakkı) ihlâl edildiğine karar vermiştir. AİHM, özellikle, başvuru sahibinin usûle ilişkin bir dizi güvenceden yararlanmış olmasına rağmen, davayı taşıdığı inceleme dairesinin, yalnızca başvuru sahibi ile başvuru sahibinin işlediği iddia edilen suçların mağdurları arasındaki ilişkiye ait verilerden ziyade, başvuru sahibinin hukuk bürosundan gelen tüm elektronik verilerin aranmasına izin verirken sadece kısa ve oldukça genel nedenler sunduğunu gözlemlemiştir. Bir hukuk bürosunda mevcut bulunan özel koşullar göz önünde bulundurulduğunda, bu şekilde kapsamlı bir aramaya izin verilmesi için özel gerekçelerin gösterilmiş olması gerekirdi. Bu tür gerekçelerin yokluğunda, tüm verilere elkoyulması ve bunların incelenmesi, meşru amaca ulaşmak için gerekli olanın ötesine geçmiştir. (Robathin - Avusturya 3 Temmuz 2012, 30457/06)

17 AİHM, Sözleşme'nin 10. maddesinin (ifade özgürlüğü) ihlâl edildiğine karar vermiştir. Raporda, gazetecilerin kaynaklarını ifşa etmeme hakkının, kaynaklarının hukuka uygunluğuna veya hukuka aykırılığına bağlı bir ayrıcalık olarak değil, en üst düzeyde dikkatle ele alınması gereken bilgi edinme hakkının hâkiki bir parçası olarak kabul edilebileceği vurgulanmıştır. Bu durumda soruşturma makamları, soruşturmanın delil sağlama konusundaki menfaatini, gazetecinin ifade özgürlüğünün korunmasına yönelik kamu menfaatine karşı doğru bir şekilde dengeleyememişlerdir. (Nagla - Letonya, 16 Temmuz 2013, 73469/10)

18 "*Delillerin doğruluğuna ilişkin herhangi bir şüpheye mahal vermemek amacıyla davanın tüm koşullarına yönelik, çekişmeli bir şekilde gerçekleştirilmesi gereken kapsamlı bir değerlendirmenin olmaması, başlı başına ilk bakışta (prima facie) AİHS Madde 6 § 1 uyarınca garanti edilen adil yargılanma hakkı gerekliliklerıyle çelişmektedir*" (Mehmet Zeki Çelebi - Türkiye, 28 Ocak 2020, No: 27582/07, § 51). Ayrıca bkz. Guide on Admissibility of Evidence in Criminal Matters – Focus on Türkiye (Cezai Konularda Delillerin Kabul Edilebilirliği – Türkiye Rehberi)

web siteleri, donanım üreticileri, yazılım geliştiricileri vb.) talep edilebilmektedir. Genellikle, abone bilgilerine erişim için gereken koşullar, trafik verilerine erişim koşullarından daha rahattır; en katı usûller ise içerik verilerine uygulanmaktadır.

Türk hukuk sisteminde, teknoloji firmalarının ve hizmet sağlayıcıların abone ve trafik verilerini saklamalarına ve bir üretim emri ile talep edilmesi hâlinde bunları adli makamlarla paylaşmalarına olanak tanıyan yasal dayanak mevcuttur. Buna dayanak teşkil eden en önemli mevzuat olan İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ("İnternet Kanunu"), içerik sağlayıcıları, yer sağlayıcıları, "erişim sağlayıcıları" olarak da adlandırılan İnternet Hizmet Sağlayıcıları, toplu kullanım sağlayıcıları ve sosyal ağ sağlayıcıları gibi internet aktörlerinin hukuki, cezai ve idari sorumluluklarını düzenlemektedir. Ayrıca Polis Vazife ve Salahiyet Kanunu Ek Madde 7'de polisin istihbarat görevleri ve siber suçlarla mücadeleye ilişkin özel bir üretim emri türü de düzenlenmiştir.

Bu bağlamda AİHM, içtihatlarında hizmet sağlayıcılardan temel haklara ilişkin iletişim verilerinin alınmasına yönelik rejimlerin risklerine dikkat çekmiş[19] ve özellikle kitlesel dinleme rejimleri için "uçtan uca koruma" şartının gerekliliğini vurgulamıştır.[20]

---

19 Büyük Daire, kitlesel dinleme rejimi bakımından Sözleşme'nin 8. maddesinin (özel hayata ve aile hayatına/haberleşmeye saygı hakkı) ihlâl edildiğine (oybirliğiyle); iletişim hizmeti sağlayıcılarından iletişim verilerinin alınmasına ilişkin rejim bakımından 8. maddenin ihlâl edildiğine (oybirliğiyle); Birleşik Krallık'ın yabancı hükümetler ve istihbarat teşkilatları tarafından dinlenen materyallerin talep edilmesi rejimi bakımından 8. Maddenin ihlâl edilmediğine (beşe karşı on iki oyla); hem kitlesel dinleme rejimi hem de iletişim hizmeti sağlayıcılarından iletişim verilerinin alınmasına ilişkin rejim bakımından Sözleşme'nin 10. maddesinin (ifade özgürlüğü) ihlâl edildiğine (oybirliğiyle) karar vermiştir (Big Brother Watch ve Diğerleri - Birleşik Krallık (BD, 25 Mayıs 2021), 58170/13, 62322/14 ve 24969/15).

20 Bahse konu dava, başvuru sahibi vakfın, İsveç'te ve yurtdışında bulunan kişi, kurum ve şirketlerle e-posta, telefon ve faks yoluyla kurduğu ve genellikle hassas konuları içeren günlük iletişiminin, sinyal istihbaratı yoluyla dinlenerek incelendiği veya inceleneceği iddiasıyla ilgilidir. Büyük Daire, ikiye karşı on beş oyla, Sözleşme'nin 8. maddesinin (özel hayata ve aile hayatına, konut ve haberleşme saygı hakkı) ihlâl edildiğine karar vermiştir. Mahkeme özellikle, İsveç'teki kitlesel dinleme rejiminin temel özelliklerinin, Sözleşmenin kanunun niteliğine ilişkin gerekliliklerini karşılamasına rağmen, rejimin yine de üç açıdan kusuru bulunduğunu tespit etmiştir: kişisel veri içermeyen dinlenen materyallerin imhâ edilmesine dair net bir kuralın bulunmaması; Sinyal İstihbarat Yasası'nda veya ilgili diğer mevzuatta, istihbarat materyalinin yabancı kurumlara iletilmesine karar verirken, bireylerin mahremiyete ilişkin menfaatlerinin dikkate alınmasına dair bir gerekliliğin bulunmaması; ve etkili bir geriye dönük incelemenin olmaması. Bu eksikliklerin bir sonucu olarak, sistem "uçtan uca" koruma şartını yerine getirmemiş, bu konuda davalı Devlete bırakılan takdir marjını aşmış ve genel olarak keyfilik ve suistimal riskine karşı koruma sağlamamıştır. (Centrum För Rättvisa - İsveç, BD, 25 Mayıs 2021, 35252/08)

Bununla birlikte, sosyal ağ sağlayıcılarının çoğu çok uluslu özel aktörler olduğundan, sınır ötesi üretim emirleri ve uluslararası iş birliği yöntemleri giderek daha önemli hâle gelmektedir.

9.2. Arama emirleri

Elektronik delillere elkoyulabilmesi ve bilgisayarda, bilgisayar kütüklerinde ve programlarında arama ve elkoyma işlemi yapılabilmesi için Ceza Muhakemesi Kanunu'nun ("CMK") 116. maddesi ve devamı niteliğindeki maddeler uyarınca, şüphelinin kullandığı cihazların tespiti ve elde edilmesi için öncelikle genel bir arama emrine ihtiyaç vardır. Şüpheli ile cihaz arasındaki bağlantı açık ise, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısı, elde edilecek materyallerin CMK 134. maddesi ve Adli ve Önleme Aramaları Yönetmeliğinin ("AÖAY") 17. maddesi kapsamında incelenmesi için karar vermelidir. Bu hükümlere göre, arama emri kararının diğer ön koşulları: i) bir soruşturmanın yürütülüyor olması, ii) somut delillere dayanan kuvvetli şüphe sebebinin varlığı, iii) başka surette delil elde etme imkanının bulunmamasıdır.

Bahsi geçen maddenin başlığından da anlaşılacağı üzere, arama ve elkoymanın yapılabileceği yer veya nesne, bilgisayar ve bilgisayar programları ile bilgisayar kütükleridir. Gelişen teknolojiler karşısında, özellikle ağ bağlantılarının bu bağlamda değerlendirilip değerlendirilemeyeceği tartışma konusu olmuştur. Yönetmelikteki bu eksiklikten kaynaklanan tartışma, AÖAY'nin 17. maddesine eklenen "*Bu işlem bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile diğer çıkarılabilir donanımları hakkında da uygulanır*" ifadesiyle çözüme kavuşturulmaya çalışılmıştır.

CMK'nın 134/2-5 maddesi usûle ilişkin bazı güvenceler sağlamaktadır. İlgili madde, kolluk kuvvetlerinin elkoyulan sistemdeki tüm verilerin yedeklemesinin yapılmasını ve alınan bu yedekten bir kopya çıkartılarak şüpheliye veya vekiline vermesini ve bu hususun tutanağa geçirilerek imza altına alınmasını gerektirmektedir[21].

21 Ancak bu gereklilik, özellikle çocuk pornografisi gibi, elde edilen suç delillerinin bir kopyasının şüpheliye geri verilmesinin suçun özüne zarar verdiği durumlarda sorun teşkil etmektedir. Bu nedenle, bu konudaki hükümlerin değiştirilmesine ihtiyaç vardır.

Yargıtay'ın çığır açan bir kararı (16. CD., E. 2019/2637 K. 2019/5904 T. 10.10.2019) CMK'nın 134. maddesinin özel karakterini ve ilgili usûli adımlarının bir ceza yargılamasında dijital delillerin kabul edilebilirliği üzerindeki etkisinin altını çizmiştir: *"Bu itibarla arama ve elkoymanın özel bir hali olarak CMK'nın 134. maddesinde düzenlenen ve özel hayatın gizliliğine daha fazla müdahale içermesi nedeniyle yasa koyucu tarafından genel arama ve elkoymadan daha sıkı koşullara tabi tutulan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama ve elkoymanın bu özelliği gözardı edilmek suretiyle, hâkimlik kararı olmaksızın aramayı gerçekleştiren kişilerce elkoyma işlemine geçildiği sırada sistemdeki verilerin yedeklemesi (imaj-adli kopya) yapılmadan ve yedekten bir kopya alınıp şüpheli veya vekiline verilmeden, ya da yukarıda yazılı nedenlerden dolayı mahalde yedekleme ve yedekten kopya verme olanağının bulunmadığının objektif olarak kabulünde zorunluluk bulunan hallerde, aramayı yapan kolluk birimince dijital delillere müdahaleyi önleyecek şekilde, seri numaraları tutanağa yazılmak suretiyle usulüne uygun olarak zapt edilip mühürlenmeden, şüpheli veya müdafiinin istemesi hâlinde nezaret etme ve denetleme imkanı sağlanarak inceleme mahalline kadar eşlik etmesi sağlanmadan ve bu yerde şüpheli veya müdafiinin hazır bulunmasına imkan verildikten sonra mümkün olan en kısa süre içinde mühür açılıp, dijital medyanın derhal imajının alınarak ilgilisine de imajlardan bir kopya ve orijinal medya teslim edilmeden, yine sanık veya müdafiinin mühür açma işlemi sırasında hazır bulunmasının mümkün olmadığı hallerde, mühür açma işleminin arama ve elkoyma kararını veren hâkimin huzurunda açılarak imaj alma işleminin bu sırada yapılması yoluna gidilmeden inceleme yapılması hâlinde arama ve elkoyma işleminin yasaya ve hukuka uygunluğundan bahsetmek mümkün olmadığı gibi bu yolla elde edilen delillerin de hukuka uygunluğu tartışılır hâle gelecek ve yargılama makamınca hükme esas alınması mümkün olamayacaktır."*

9.3. Arama ve elkoyma sırasında dikkat edilmesi gereken hususlar

Soruşturmayı yürüten cumhuriyet savcısının arama ve elkoyma emrinin yerine getirilmesine ilişkin talimatları ayrıntılı ve net olmalıdır. Siber suçlarda delil toplamadaki başarı oranının artması, siber suçlarla mücadelenin önemli bir göstergesidir. Elektronik delillerin güvenilir bir şekilde eksiksiz tespiti ve zarar görmeden toplanması, olay yerine ilk müdahalenin uygun şekilde

yapılması ile mümkündür. Buna paralel olarak, delillerin toplanması özel bir uzmanlık gerektirmektedir. Bu nedenle, siber suçlarla ilgili arama ve elkoyma süreçlerinde görevlendirilecek kolluk personelinin gerekli bilgi ve teknik kapasiteyle donatılmış olması gerekmektedir.

Ev/ofis binalarında arama yapılırken, önemli delillerin atılması/imhâ edilmesi veya şüphelilerin bilgisayar sistemlerine, bilgisayar verilerine ve dijital cihazlara elkoyulacak olan olay yerini terk etmesi riskini ortadan kaldırmak amacıyla, ilgili konuma erişmek için kullanılabilecek tüm yolların arama öncesinde güvenlik altına alınması gerekir.

Dijital veriler oldukça uçucudur ve bu nedenle olay yerine giriş hızına dikkat edilmelidir. Şüphelinin giriş sırasında verileri silmesinin/ortadan kaldırmasının/imhâ etmesinin önlenmesi önemlidir ve şüphelinin dijital delil içerebilecek herhangi bir cihazdan uzak tutulması için adımlar atılmalıdır.

Bilgisayar sistemlerine, bilgisayar verilerine ve dijital cihazlara elkoyulacağı bir yere girildikten sonra aşağıdaki işlemlerin ivedilikle yapılması önerilir:

- Olay yerinde bulunan bilgisayar sistemlerinin sayısının, türlerinin, bir ağa bağlı olup olmadıklarının ve internete erişip erişemeyeceklerinin tespit edilmesi ve belirlenmesi.
- İşlemin/aramanın gerçekleşeceği yerde tespit edilen kişilerin, bilgisayar sistemlerine/verilerine, dijital cihazlara veya diğer elektronik ekipmanlara ve ayrıca güç kaynaklarına erişiminin engellenmesi.
- Olay yerinin, elkoyulması hedeflenebilecek tüm dijital delil kaynaklarının, bunların durumlarının ve bağlantılarının belgelenmesi.
- Bilgisayar sistemlerini, bilgisayar verilerini ve dijital cihazları kullanırken, görünmeyen izlere zarar vermemek ve parmak izi/DNA delillerinin başarılı bir şekilde toplanmasını sağlamak amacıyla koruyucu eldiven kullanılması.
- Tespit edilen bilgisayar sistemlerinin her birinin çalışma durumunun kontrol edilmesi:

- bilgisayar sistemi kapalıysa, açılmaması; koşullar sistemin yerinde analizini gerektiriyorsa, orijinal diskin bütünlüğünü korumak için, orijinal diskin adli bir klonunu kullanarak veya bir yazma-koruma/yazma-önbellekleme mekanizması kullanarak sistemin başlatılması önerilir.

- bilgisayar sistemi çalışıyorsa, canlı veri toplamanın yapılıp yapılmayacağı kontrol edilmelidir. Bunun ardından, işletim sistemine bağlı olarak bilgisayar sistemi kapatılabilir.

Uygulamalar, arama yapılan konumun, bilgisayar sistemlerinin, bilgisayar verilerinin ve dijital cihazların müteakip analizini desteklemek için başka veri ve bilgiler sağlayabileceğini göstermiştir. Elektronik olmayan, ancak ilgili olabilecek delillere örnek olarak yazılı parolalar ve diğer el yazısı notlar, bir önceki sayfaya yazılan yazıların izinin alttaki boş sayfaya geçtiği kâğıt defterler (bu izlerin üzeri kurşun kalemle boyanmamalıdır), sanal para birimleri için kâğıt cüzdanlar, donanım ve yazılım kılavuzları, metin veya grafik bilgisayar çıktıları, fotoğraflar veya soruşturmalarda yararlı olabilecek kişisel ilgi alanlarıyla ilgili bilgiler verilebilir.

9.4. Adli Bilişim - Süreçlere genel bakış

Adli tıp bilimi, herhangi bir alanın hukuki konularla ilgili olarak incelenmesidir. Adli deliller ise daha spesifik olarak, mahkemede kabul edilebilirlik için katı güvenilirlik ve bilimsel bütünlük standartlarını karşılayan delilleri ifade eder. Adli Bilişim, mahkemede kabul edilebilirlik amacıyla bilgisayar sistemlerinde, dijital cihazlarda ve diğer depolama ortamlarında depolanan delillerin ele geçirilmesi, işlenmesi, analizi ve raporlanması ile ilgili bir adli tıp dalıdır.

Adli Bilişimin dâhil olduğu bir vakada standart usûl genellikle beş adımdan (tespit, toplama, ele geçirme, analiz ve raporlama) oluşur.

Cihazların tespiti ve toplanması yukarıda yer alan arama ve elkoyma bölümünde açıklanmıştır.

"Ele geçirme", genellikle dijital bir cihazda depolanan verilerin adli bilişim görüntüsünü elde etmek için uzman bir yazılım kullanılarak dijital delillerin elde edilmesidir. Bu, soruşturmayı yürütenlerin başka kaynaklardan adli olarak veri elde etmesi gereken durumlarda, bir arama ve elkoyma işleminde uçucu verilerin elde edilmesiyle, elkoyulan bir bilgisayardan şüphelinin sabit diskinin görüntülenmesiyle veya başka herhangi bir süreç aracılığıyla gerçekleşebilir.

Bu erken aşamada geri dönüşü olmayan birçok hata yapılabileceğinden, ele geçirme adımı çok önemlidir. Delil zincirinin bozulmaması, tüm adımların belgelenmesi ve ele geçirilen her şeyin doğrulanması önemlidir.

Adli bilişim uzmanları da verilerin işlenmesini değerlendirecektir. Elektronik delillerin işlenmesi, zaman, etkinlik veya büyük veri hacimleri söz konusu olduğunda oldukça önemlidir. Bu adımda adli bilişim uzmanları belirli cihazlara veya verilere öncelik verebilir, akıllı ve vakaya özgü filtreler uygulayabilir (Veri Madenciliği) veya görüntüyü normal bir soruşturmacının analiz edebileceği şekilde işleyebilirler (örneğin, silinen dosyaları kurtararak, kapsayıcıları (konteynerleri) devreye alarak, şifrelemeyi kırarak, internet geçmişi, sohbet kütükleri ve benzeri uygulama verilerini ayrıştırarak).

"Analiz", yetkin bir adli bilişim uzmanının adli bilişim görüntüleri üzerinde elektronik delil aramasıdır. Bu adım oldukça zaman alıcı olabilir ve izleri ve görüntü üzerindeki bozuklukları yorumlamak için ciddi uzmanlık bilgisi gerektirebilir. Adli bilişim uzmanları, bu adımları tamamlamak için genellikle sertifikalı adli bilişim yazılımı kullanırlar. Bu yazılım, tanımlanmış kelimelerin, dosyaların, resimlerin veya davayla ilgili olduğu düşünülen diğer verilerin aranmasına olanak tanır. Bu işlem adli bilişim uzmanı tarafından gerçekleştirilse de soruşturmacı ve cumhuriyet savcısı da, aşağıda Bölüm 9.5'te açıklandığı üzere önemli bir rol oynar.

"Raporlama". Tüm deliller analiz yoluyla tespit edildikten sonra, mahkemede kullanılmak üzere kopyalanmalıdır. Bu adımda adli bilişim uzmanının dava için bir rapor hazırlaması gerekir. Uzmanın buradaki rolü, hâkim ve cumhuriyet savcılarına, karmaşık teknik bağlamları ve hangi delillerin bulunduğunu, nerede bulunduğunu, nasıl bulunduğunu ve oraya nasıl/ne zaman gelmiş olabileceğini kolayca anlayabilecekleri şekilde göstermek ve açıklamaktır.

9.5. Cumhuriyet Savcısı ve Hâkimlerin Adli Bilişim İnceleme Talepleri

Adli bilişim çerçevesinde elektronik delil toplanması ve saklanması süreçlerine ilişkin bilgiler önceki bölümlerde ele alınmıştır.

Dijital cihazların adli bilişim incelemesi ve bunlardan veri alınması genellikle adli bilişim laboratuvarlarında gerçekleştirilir. Dijital adli görüntü elde edildikten sonra analiz ve raporlama aşamalarına geçilir. Yukarıda da belirtildiği gibi, cumhuriyet savcısı ve soruşturmacılar, adli bilişim uzmanına net talimatlar sağlanmasında önemli bir role sahiptir. Birçok adli bilişim laboratuvarında, cumhuriyet savcısı veya soruşturmacı inceleme için cihazları teslim ettiğinde doldurulması gereken şablon belgeleri bulunmaktadır. Bu belgelerin (veya

yazılı taleplerin) doğru bir şekilde doldurulması, adli görüntünün doğru şekilde analiz edilmesi için çok önemlidir.

Bir cumhuriyet savcısı veya soruşturmacının net talimatlar vermediği durumlarda, adli bilişim uzmanı deliler üzerinde gereksiz analizler yapabilir ve önemli materyalleri araştırmayabilir. Talimatların iletilmesinde yaşanan bu tarz eksiklikler genellikle ilave maliyetlere, gecikmelere ve hatalı raporlara neden olmaktadır.

Şablon belgeleri (veya yazılı talepler) soruşturmanın doğru bir özetini içermelidir. Mağdurlar, şüpheliler, ilgili olaylar, tarihler, saatler ve diğer göze çarpan bilgiler gibi ayrıntılar özete dâhil edilmelidir. Belgede (veya yazılı talepte), işlem kayıtları, görüntü türleri, dolandırıcılığın ayrıntıları vb. gibi tam olarak neyin arandığı tanımlanmalıdır ve bu hususlar ana hatlarıyla belirtilmelidir. Analizde kullanılan adli bilişim yazılımı, incelemeyi yapan uzmanın kelime araması yapmasına olanak tanır. Örneğin, vaka kredi kartı dolandırıcılığı ile ilgiliyse, incelemeyi yapan uzman 16 basamaklı sayısal dizileri aratabilir ve vaka belirli bir e-posta hesabıyla ilgiliyse, uzman, kelime araması yaptırarak bu tür olaylara ilişkin tüm kayıtları bulabilir. Soruşturmacı ve/veya cumhuriyet savcısı, incelemeyi yapan uzmanın araştırmasında kullanabileceği ilgili arama terimlerini belirlemelidir.

AİHM, *Kırdök ve Diğerleri* - Türkiye (3 Aralık 2019, No:14704/12), Trabjo Rueda - İspanya (30 Mayıs 2017, no: 32600/12) ve Särgava - Estonya (16 Kasım 2021, 698/19) kararlarında elektronik delillerin arama ve elkoyma süreçleri ile bu delillere yönelik adli bilişim süreçleri için özel talimatlar da dâhil olmak üzere usûli güvencelere yönelik ihtiyaca vurgu yapmıştır.

Raporlama, söz konusu inceleme için hangi bulguların kullanılabileceğinin belirlenmesi ve bu bilgilerin bu doğrultuda adli makamlara sunulmasıdır. Ancak tam da bu nedenle, adli makamlar olan hâkimler ve cumhuriyet savcıları nihai bir teknik görüşe ulaşmak için, teknik raporu hazırlayacak adli bilirkişiye, suçun olgusal arka planı, elektronik ve diğer delillere ilişkin yapılacak analizin kesin kapsamı ve açık talimatlar ve sorular da dâhil olmak üzere net bir çerçeve çizmelidir. CMK'nın 62 ilâ 68. maddeleri, bilirkişiler için uygulanacak usûli çerçeveyi düzenlemektedir. Adli makamlar ayrıca, kendi özel hükümlerine göre kolluk ve jandarma kriminal laboratuvarları ile Adli Tıp Kurumundan bilirkişi görüşü isteyebilirler.

Sonuç olarak sunulan raporda, dijital delillerin nasıl elde edildiğinin teknik yönü ve hangi adli bilgi edinme yöntemlerinin kullanıldığı da anlaşılır bir dille belirtilmelidir. Raporda ayrıca olayla ilgili bilgiler, araştırmanın yapıldığı zaman dilimi, incelenen elektronik deliller, inceleme sırasında kullanılan yazılım ve donanımlara ilgili bilgiler, inceleme sırasında kullanılan yöntemler ve araştırma sonucunda elde edilen bulgular da yer almalıdır. Sonuç olarak, dijital adli bilirkişi raporları hukuka uygun ve denetlenebilir olmalıdır.

10. Siber suç soruşturmalarında uluslararası iş birliği talepleri

Yetkili makamlar ve çok uluslu hizmet sağlayıcılar arasındaki iş birliği, elektronik delillerin elde edilmesinde esastır. Türkiye için uluslararası iş birliği çok taraflı anlaşmalara (Budapeşte Sözleşmesi, Varşova Sözleşmesi) veya ikili anlaşmalara dayanabilir ve bu tarz sözleşmelerin olmadığı hallerde uluslararası örf ve âdet hukuku kuralları veya mütekabiliyet ilkesi çerçevesinde yürütülmelidir.

Budapeşte Sözleşmesinin 7/24 İrtibat Ağı (madde 35 kapsamında oluşturulmuştur), bilgisayar sistemleri ve verilerle ilgili suçlara yönelik soruşturma veya kovuşturmalar amacıyla doğrudan bilgi alışverişi ve yardım için veya bir suça ilişkin elektronik formatta delil toplanması bakımından kritik bir rol oynamaktadır. Bu irtibat noktalarının genel amaçları, uluslararası iş birliğini kolaylaştırmak, diğer irtibat noktalarına teknik danışmanlık vermek, verilerin hızlı bir şekilde korunması için uygun mekanizmayı harekete geçirmek, delilleri (depolanan veriler ve trafik verileri) ivedilikle toplamak ve şüphelileri tespit etmek ve ortaya çıkartmaktır. 35. Maddenin uygulanması ancak Emniyet Genel Müdürlüğü bünyesindeki 7/24 Tek İrtibat Noktası aracılığıyla gerçekleştirilir.

Tüm bunlar, sadece acil nedenlerle bir koruma tedbiri olarak uygulanır ve saklanan verilerin otomatik olarak açıklanacağı anlamına gelmez. Örneğin mütekabiliyet kuralları göz önüne alındığında, çoğu ülkede buna cezai sorumluluk yükleyen yasal dayanaklar veya standartlar olmadığından, Türk makamlarının hakaret davalarına yönelik ilettiği üretim emirlerinin bu ülkeler tarafından yerine getirilmeyeceği unutulmamalıdır.

Uluslararası iş birliğini sağlamaya yönelik diğer yöntemler arasında, başka yöntemlerin yanı sıra, Interpol, Europol, EuroJust, ikili polis ilişkileri ve Küresel Savcılar Elektronik Suç Ağı (Uluslararası Savcılar Birliği bünyesinde)[22] yer almaktadır.

22 https://www.iap-association.org/GPEN/Home

Bu proje Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.
This Project is co-funded by the European Union and the Council of Europe.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Bu Kılavuz "Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi İhlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması" Avrupa Birliği ve Avrupa Konseyi Ortak Projesi kapsamında hazırlanmıştır.

Bu Proje Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmekte, Avrupa Konseyi tarafından yürütülmektedir. Projenin yararlanıcı kurumları Türkiye Cumhuriyeti Adalet Bakanlığı Ceza İşleri Genel Müdürlüğü ve Türkiye Adalet Akademisidir. Projenin sözleşme makamı Merkezi Finans ve İhale Birimidir.

Avrupa Konseyi, Avrupa kıtasının önde gelen insan hakları kuruluşudur. Kuruluş bünyesinde 46 üye devlet bulunmaktadır. Avrupa konseyi üye devletlerinin tamamı; insan hakları, demokrasi ve hukukun üstünlüğünün korunmasını teminat altına almak üzere tasarlanmış olan Avrupa İnsan Hakları Sözleşmesi'ni imzalamıştır. Avrupa İnsan Hakları Mahkemesi, Sözleşme'nin üye devletlerdeki uygulanmasını denetler.