Uluslararası Bilişim Sistemleri ve Uygulamaları Dergisi
International Journal of Information Systems and Applications

https://dergipark.org.tr/pub/ubsud

İnceleme Makalesi		Cilt No:	1	Sayı No:	1
Geliş Tarihi:	10.05.2025	Kabul Tarihi:	02.06.2025	Yayın Tarihi:	06.06.2025

BULUT ORTAMINDA ADLİ İNCELEME: KANITIN NEREDE BAŞLAYIP NEREDE BİTTİĞİNİN BELİRLENMESİ

Zeynep ÇELİK [1]

Özet

Bu makale, bulut bilişim teknolojilerinin adli bilişim süreçlerine etkilerini, sunduğu faydalar ve getirdiği zorluklar (fiziksel erişim eksikliği, veri uçuculuğu, yasal karmaşa) çerçevesinde incelemektedir. Olay müdahalesi ve dijital delil toplamanın bulutta nasıl farklılaştığı analiz edilirken, 'bulutta kanıt nerede başlar, nerede biter?' sorusuna metodolojik bir çözüm olarak özgün Bulutta Kanıt Yaşam Döngüsü Modeli (CELM) ve Kanıtın Erişilebilirlik ve Bütünlük Skalası (KEBS) sunulmaktadır. LastPass veri ihlali vakası üzerinden bu modeller ışığında adli inceleme adımları ve karşılaşılan sorunlar değerlendirilmiştir. Çalışma, bulut sistemlerinin adli bilişim açısından yeniden değerlendirilmesi, önerilen modellerin bu sürece katkısı ve kurumsal hazırlığın artırılması gerektiğini vurgulamaktadır.

Anahtar Kelimeler: Bulut Bilişim, Adli Bilişim, LastPass, Olay Müdahalesi, Veri Güvenliği, Bulut Adli Bilişimi

FORENSICS INVESTIGATION IN THE CLOUD: DETERMINING WHERE EVIDENCE STARTS AND ENDS

Abstract

This article examines the effects of cloud computing technologies on digital forensics processes within the framework of their benefits and challenges (such as lack of physical access, data volatility, and legal complexities). While analyzing how incident response and digital evidence collection differ in the cloud, this study introduces the original Cloud Evidence Lifecycle Model (CELM) and the Evidence Accessibility and Integrity Scale (KEBS) as a methodological solution to the question of 'where evidence begins and ends in the cloud.' Forensic investigation steps and encountered issues are evaluated in light of these models through the LastPass data breach case. The study emphasizes the need for reassessing cloud systems from a digital forensics perspective, the contribution of the proposed models to this process, and the importance of enhancing organizational preparedness.

Keywords: Cloud Computing, Digital Forensics, LastPass, Incident Response, Data Security, Cloud Forensics

[1] Adli Bilişim Mühendisi, Gazi Üniversitesi, Bilişim Enstitüsü, zeyneppcelikk5@gmail.com, https://orcid.org/0009-0002-6095-5418

1. GİRİŞ

Kurumların hızla dijitalleşmesi, bilgi teknolojileri altyapılarını geleneksel sistemlerden bulut tabanlı yapılara doğru dönüştürmektedir. Bulut bilişim, internet üzerinden sağlanan bilgi teknolojileri hizmetlerini tanımlar (Furht & Escalante, 2010). Bu dönüşüm, veri depolama ve işleme süreçlerini büyük ölçüde bulut bilişim altyapılarına taşırken, adli bilişim (digital forensics) alanında çeşitli fırsatlar (Reilly vd., 2013) sunmanın yanı sıra veri güvenliği, mahremiyet ve hukuki sorumluluklar gibi yeni sorunları da beraberinde getirmiştir (Grobauer vd., 2011). Geleneksel fiziksel cihazlara yönelik adli incelemeler, yerini sanal ortamlarda gerçekleştirilen daha karmaşık ve dinamik süreçlere bırakmaktadır (Emekci vd., 2016).

Bulut ortamlarında adli bilişim, verilerin tek bir donanımda değil, çoklu lokasyonlarda ve sanallaştırılmış yapılar içinde barındırılması (Quick vd., 2013), fiziksel erişimin sınırlı olması ve Bulut Hizmet Sağlayıcılarının (CSP) politikalarına bağımlılık gibi nedenlerle geleneksel yöntemlerden daha karmaşık bir hale gelebilir (Emekci vd., 2016; Ruan vd., 2011). Bu karmaşıklık, "bulut ortamında kanıtın nerede başlayıp nerede bittiği" temel sorusunu gündeme getirmektedir. Bu çalışma, bulut ortamındaki adli incelemelerin özgün zorluklarını ve fırsatlarını analiz ederek bu soruya mevcut literatür ve bir vaka analizi ışığında cevap arayarak literatürdeki belirli bir boşluğu doldurmayı ve bu alandaki anlayışa özgün bir katkı sunmayı amaçlamaktadır.

Bu sorunsala metodolojik bir yanıt sunabilmek amacıyla, özgün iki yaklaşım geliştirilmiştir: Birincisi, bulut ortamındaki dijital kanıtın oluşumundan sonlanmasına kadar olan süreci bütüncül bir bakış açısıyla ele alan Bulutta Kanıt Yaşam Döngüsü Modeli (CELM)'dir. İkincisi ise, bu yaşam döngüsü içerisinde elde edilen kanıtların adli bilişim açısından güvenilirliğini ve kullanılabilirliğini değerlendirmek üzere tasarlanan Kanıtın Erişilebilirlik ve Bütünlük Skalası (KEBS)'tir. Bu modellerin, bulut adli bilişimi alanındaki mevcut boşluğu doldurarak hem teorik anlayışa hem de pratik uygulamalara katkı sağlaması hedeflenmektedir. Çalışmada ayrıca, bulut ortamında gerçekleştirilen adli incelemelerde karşılaşılan teknik, hukuki ve etik zorluklar ele alınmakta (Herman et al., 2014), kullanılan yöntemler ve araçlar tartışılmakta ve LastPass vakası üzerinden bir vaka analizi sunulmaktadır (LastPass, 2023).

Kurumların, bulut bilişimin sunduğu operasyonel ve maliyet avantajları nedeniyle bu teknolojilere hızla yönelmesi, veri güvenliği, yasal uyumluluk ve olay müdahalesi gibi kritik alanları da beraberinde etkilemektedir (Alenezi, 2021).

Sonuç olarak, bulut bilişim ve adli bilişim, günümüzün teknoloji dünyasında birbirini tamamlayan iki önemli alan haline gelmiştir. Bulut ortamlarında dijital delil toplama ve analiz etme süreçleri, daha fazla dikkat ve uzmanlık gerektiren bir alan olarak karşımıza çıkmaktadır (Zawoad & Hasan, 2014). Ayrıca, bulutun sağladığı avantajları tam anlamıyla kullanabilmek için bu yeni nesil altyapılarda adli bilişim süreçlerini de yeniden tasarlamak gerekmektedir (Peterson & Shenoi, 2013).

2. CLOUD SİSTEMLERİNİN ADLİ BİLİŞİM AÇISINDAN SUNDUĞU FAYDALAR

Son yıllarda kurumların dijitalleşme süreçlerinin hızlanmasıyla birlikte, bulut tabanlı sistemlerin kullanımı daha da yaygınlaşmıştır. Bu hızlı dönüşüm, adli bilişim (digital forensics) alanında da yeni fırsatlar ve zorluklar doğurmuştur (Reilly vd., 2013). Bulut ortamlarındaki adli bilişim süreçleri, geleneksel sistemlere kıyasla veri güvenliği, maliyet etkinliği, esneklik, veri yedekleme ve daha hızlı olay müdahalesi gibi belirgin avantajlar sunar. (Grispos vd., 2014).

2.1. Esneklik ve Ölçeklenebilirlik

Bulut bilişim sistemlerinin en büyük avantajlarından biri, esneklik ve ölçeklenebilirlik sunmasıdır (Furht & Escalante, 2010). Bulut ortamlarında, kullanıcılar ihtiyaçlarına göre kaynakları hızla artırabilir veya azaltabilirler.

2.2. Merkezi Erişim ve Veri Yedekleme

Bulut tabanlı sistemler, verilerin merkezi bir ortamda depolanmasını sağlar. Bu da adli bilişim uzmanlarının dijital delillere uzaktan erişmesini kolaylaştırır (Quick vd., 2013). Fiziksel cihazlar üzerinden yapılan adli incelemelerde, verilerin bulunduğu cihazın fiziksel olarak bulunması gerekebilir. Oysa bulut ortamlarında, dijital delillere dünyanın herhangi bir yerinden, güvenli erişim yöntemleri aracılığıyla ulaşılabilir. Bu da adli inceleme süreçlerini hızlandırır ve daha geniş bir coğrafi alanda yapılan incelemelerde esneklik sağlar.

Ayrıca, bulut sistemlerinde otomatik veri yedekleme ve çoğaltma işlemleri yapılabilir. Bu sayede dijital delillerin kaybolma riski azalır. Veriler farklı coğrafi bölgelerdeki veri merkezlerinde yedeklenebilir, bu da herhangi bir felaket durumunda bile delillerin güvenli bir şekilde korunmasını sağlar.

2.3. Güvenlik Önlemleri

Bulut sağlayıcıları, genellikle güvenlik standartlarına büyük önem verirler ve bu standartlar genellikle fiziksel donanımlara sahip yerel veri merkezlerinden daha kapsamlı olabilir (Grispos vd., 2014; Alenezi, 2021). Bulut ortamlarında, veriler güçlü şifreleme yöntemleriyle korunabilir ve erişim kontrolleri daha sıkı bir şekilde uygulanabilir. Veri şifreleme, özellikle bulut ortamlarındaki hassas bilgilerin güvenliği açısından kritik öneme sahiptir. Adli bilişim açısından, verilerin şifreli bir şekilde saklanması, hukuki süreçlerde verilerin güvenliğini ve geçerliliğini sağlayarak, olası manipülasyonlardan veya tahrifatlardan korunmasını mümkün kılar.

Ayrıca, bulut sağlayıcıları genellikle gelişmiş güvenlik protokolleri ve izleme araçları sunarlar (Aksakallı, 2019). Gerçek zamanlı güvenlik olayları izleme ve

alarm sistemleri sayesinde, adli bilişim süreçlerinde olası veri ihlalleri ve güvenlik açıkları erken bir aşamada tespit edilebilir.

2.4. Düşük Maliyet ve Kaynak Verimliliği

Geleneksel fiziksel altyapılarda, donanım ve yazılım kaynaklarının satın alınması, kurulumu ve bakımı gibi yüksek maliyetler söz konusudur. Bulut bilişim, bu yüksek başlangıç maliyetlerini ortadan kaldırarak kurumlara daha düşük işletme giderleri (OPEX) sağlar (Furht & Escalante, 2010). Bulut tabanlı çözümler, sadece ihtiyaç duyulan kaynaklar için ödeme yapılmasını sağlayarak, maliyet verimliliği sunar.

Ayrıca, CSP'ler, altyapı bakımını kendileri üstlendikleri için, adli bilişim uzmanlarının donanım sorunlarıyla ilgilenmesine gerek kalmaz ve bu da zaman tasarrufu sağlar.

2.5. Hızlı Olay Müdahalesi ve Daha Kapsamlı Veri Analizi

Bulut bilişim, adli bilişim süreçlerinde önemli bir dönüşüm yaratmaktadır (Emekci vd., 2016). Özellikle veri işleme ve analiz hızının önemli ölçüde artırılması, büyük veri setlerinin hızlı ve verimli bir şekilde işlenmesi, bu dönüşümün temel faydaları arasında yer almaktadır. Bulut bilişim altyapılarının sunduğu geniş işlem kapasitesi ve esnek kaynak yönetimi, adli bilişim uzmanlarının, geleneksel veri işleme yöntemlerine kıyasla çok daha hızlı ve etkili analizler gerçekleştirmelerini sağlamaktadır (Zawoad & Hasan, 2014).

Bulut bilişim altyapılarının en önemli özelliklerinden biri, büyük veri kümelerinin paralel işlem gücüyle işlenmesidir. Bu yaklaşım, birden fazla veri kaynağından gelen verilerin bağımsız bir şekilde eş zamanlı olarak işlenmesine imkan tanır. Bu paralel işlem gücü, çok büyük veri setlerinin daha verimli bir şekilde analiz edilmesini mümkün kılmaktadır. Örneğin, bir siber saldırı olayı sırasında, saldırıya ait dijital delillerin (log dosyaları, ağ trafiği, cihaz meta verileri vb.) hızlı bir biçimde toplanması ve bu verilerin birbirleriyle ilişkilendirilmesi gerekebilir. Bulut bilişim, bu süreci hızlandırarak adli bilişim uzmanlarının olayın kapsamını daha hızlı anlamalarına olanak tanır.

Bir diğer önemli avantaj ise, bulut bilişim altyapılarında yer alan makine öğrenmesi (Machine Learning - ML) ve yapay zeka (Artificial Intelligence - AI) tabanlı analitik araçlarının kullanımıdır. Bu araçlar, adli bilişim uzmanlarının veri kümeleri içindeki anormallikleri tespit etmelerine ve potansiyel suç faaliyetlerini belirlemelerine olanak sağlar.

Bulut bilişim, verinin yalnızca depolanmasını değil, aynı zamanda anlamlı bir şekilde analiz edilmesini sağlayacak gerekli araçları da sunmaktadır (Big Data Bilişim, 2025). Bu süreç, adli bilişim uzmanlarının veriyi daha etkili bir şekilde incelemelerine olanak tanır. Özellikle büyük veri analitiği (Big Data Analytics) ve veri görselleştirme (Data Visualization) gibi gelişmiş teknolojiler, geniş veri

setlerinde anlamlı ilişkiler ve desenler ortaya çıkarılmasına yardımcı olur. Bu teknolojiler sayesinde, adli bilişim uzmanları daha doğru ve hızlı sonuçlara ulaşabilirler.

3. CLOUD SİSTEMLERİNİN ADLİ BİLİŞİM AÇISINDAN SUNDUĞU ZORLUKLAR

Bulut bilişimin yaygınlaşması, veri işlemede avantajlar sağlarken, adli bilişim süreçlerinde yeni zorlukları da beraberinde getirmiştir. Fiziksel erişim eksikliği, uçucu veri yapısı, karmaşık telemetri verileri ve paylaşılan sorumluluk modeli gibi etkenler, dijital delillerin toplanmasını ve analizini güçleştirerek hem teknik hem de hukuki açıdan soruşturma süreçlerini zorlaştırmaktadır.

3.1. Fiziksel Erişim Sınırlamaları

Bulut sistemlerinde veriler genellikle CSP'lerin denetiminde bulunan, coğrafi olarak dağılmış uzak sunucularda depolanmaktadır (Quick vd., 2013). Bu durum, geleneksel adli bilişim süreçlerinde alışık olunan fiziksel erişim imkânını ortadan kaldırmakta ve delil toplama süreçlerini önemli ölçüde karmaşıklaştırmaktadır (Herman et al., 2014; Ruan vd., 2011).

Adli bilişim uzmanları, bulut ortamında çalışan sanal makineler (Virtual Machines - VM), sanal ağ yapıları ve dağıtık depolama sistemlerine doğrudan erişim yetkisine sahip değildir. Bu da, özellikle olay müdahalesi sırasında veriye erişim sağlanmasını zorlaştırır. Örneğin, bir fiziksel sunucuya el koyma işlemi bulutta mümkün olmadığından, uzmanlar CSP'nin işbirliğine ve sağladığı arayüzlere bağımlı kalır. Ayrıca, sistem yöneticisi veya CSP'nin işbirliği olmadan, kanıtların güvenli bir şekilde elde edilmesi, doğrulanması ve zincirleme delil (chain of custody) sürecine uygun şekilde elde edilmesi çoğu zaman mümkün olmamaktadır (Emekci vd., 2016). Bu durum, aşağıdaki örnek olayda da görülebileceği gibi, soruşturma süreçlerini yavaşlatabilir.

Dropbox ve FBI Soruşturması

2012 yılında Federal Bureau of Investigation (FBI)'ın yürüttüğü bir soruşturmada, bir kullanıcının yasa dışı dosya paylaşımı yaptığı iddiasıyla Dropbox'taki verilerine erişilmesi gerekmişti. Soruşturma sürecinde, Dropbox'un Amerika Birleşik Devletleri'nde yer alan veri merkezlerinde saklanan dosyalara, şirketin doğrudan işbirliğiyle erişilebilmiştir. Bu durum, olay yerinin fiziksel olarak belirlenememesi ve verilerin farklı yargı bölgelerinde dağılmış olması nedeniyle erişim izinleri ve yasal prosedürlerin aylarca sürmesine yol açmıştır.

3.2. Dinamik ve Uçucu Veri Yapısı

Bulut ortamları, bilişim kaynaklarını dinamik bir şekilde yönetir; VM'ler, konteynerler ve ağ bileşenleri anlık olarak başlatılabilir, durdurulabilir, silinebilir veya farklı fiziksel ortamlara taşınabilir (Furht & Escalante, 2010). Bu esneklik, sistemde üretilen verilerin uçucu (volatile) nitelikte olmasına neden olur (Herman et al., 2014). Özellikle sanal makinelerde çalışan geçici oturumlar ile RAM tabanlı veriler, yalnızca belirli bir zaman aralığında erişilebilir durumdadır. Bu tür veriler, olaydan kısa bir süre sonra silinebilir, üzerine yeni veriler yazılabilir ya da sistem yeniden başlatıldığında tamamen kaybolabilir.

Adli bilişim açısından, bu tür geçici verilerin zamanında tespit edilerek toplanması büyük önem taşır. Ancak, olayın fark edilmesi ve müdahale edilmesi arasında geçen sürede bu verilerin kaybolma ihtimali, delil bütünlüğünü ciddi şekilde riske atar. Bu durum, aşağıdaki Amazon EC2 örneğinde somutlaşmaktadır.

Amazon EC2 Otomatik Yeniden Başlatmalar

Amazon EC2 (Elastic Compute Cloud) hizmetinde, belirli sistem arızalarında sanal makineler otomatik olarak yeniden başlatılır. Bu süreçte, bellekte tutulan uçucu veriler tamamen silinir. 2020 yılında yaşanan bir oltalama saldırısında, saldırganın komut çalıştırmak için EC2 örneğine sızdığı ancak olayın fark edilip müdahale edilene kadar sistemin yeniden başlatıldığı ve tüm RAM verilerinin kaybolduğu raporlanmıştır. Bu durum, saldırının nasıl gerçekleştiğine dair kritik bilgilerin elde edilmesini engellemiştir.

3.3. Bulut Telemetri Verilerinin Toplanması ve Analizindeki Zorluklar

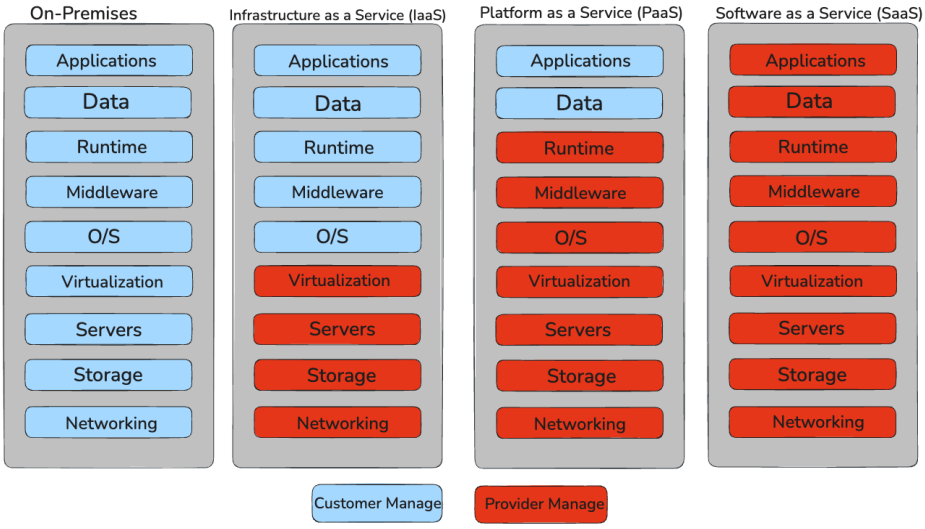
Bulut ortamları, büyük miktarda telemetri verisi (loglar, metrikler, olay kayıtları vb.) üretir. Ancak bu verilerin adli bilişim amaçlı toplanması ve analizi çeşitli zorluklar içerir (Herman et al., 2014). Bunlar arasında veri yapılandırmasının (Configuration) karmaşıklığı, içeriğin (Content) tam olarak ne ifade ettiğinin anlaşılması, olayların zamanlamasındaki (Timing) senkronizasyon sorunları, verinin yapısındaki (Structure) farklılıklar, farklı kaynaklardan gelen verilerdeki çeşitlilik (Variance) ve veri saklama (Retention) politikalarının CSP'ler arasında ve hatta aynı CSP'nin farklı servislerinde değişiklik göstermesi sayılabilir. Bu faktörler, tutarlı ve bütüncül bir kanıt zinciri oluşturmayı zorlaştırabilir.

3.4. Paylaşılan Sorumluluk Modeli

Bulut hizmet sağlayıcıları ile kullanıcılar arasında, güvenlik ve yönetim açısından sorumlulukların bölüştürüldüğü bir yapı olan Paylaşılan Sorumluluk Modeli (Shared Responsibility Model) benimsenmiştir (Grispos vd., 2014) (bkz. Şekil 1). Bu modele göre, CSP'ler altyapının güvenliği, fiziksel sunucu koruması, ağ güvenliği ve bazı şifreleme işlemlerinden sorumludur. Kullanıcılar ise işletim sistemleri, uygulama

seviyesi güvenlik, erişim kontrolü ve log yönetimi gibi servisleri yönetmekle yükümlüdür (Alenezi, 2021).

Paylaşılan Sorumluluk Modeli, bulut hizmet türüne bağlı olarak farklılık gösterir. En temel hizmet modeli olan Altyapı Hizmeti (Infrastructure as a Service - IaaS)'de, kullanıcılar işletim sistemlerinden uygulamalara kadar daha geniş bir yelpazede sorumluluk taşırken, bulut sağlayıcı yalnızca fiziksel altyapıdan sorumludur. Platform Hizmeti (Platform as a Service - PaaS)'te, uygulama geliştirme altyapısı sağlayıcı tarafından sunulduğundan, kullanıcı sadece geliştirilen uygulamanın güvenliğinden ve veri yönetiminden sorumludur. Yazılım Hizmeti (Software as a Service - SaaS) modelinde ise kullanıcı genellikle sadece veri girişi ve erişim kontrolünden sorumludur; uygulamanın altyapısı ve güvenliği tamamen hizmet sağlayıcının yükümlülüğündedir. (bkz. Şekil 1.) Bu farklılıklar, adli bilişim süreçlerinde hangi tarafın hangi veriye erişebileceği ve hangi seviyede müdahalede bulunabileceği konusunda belirleyici olabilir (Ruan vd., 2011).



Şekil 1. Bulut Yönetim Sorumluluğu

Bu yapı, adli incelemelerde hangi tarafın hangi veriye erişimi olduğu, verilerin nasıl işlendiği ve sorumluluğun kime ait olduğu gibi soruları gündeme getirir. Bulut ortamlarında, çok sayıda müşteri (veya "kiracı"), aynı fiziksel alt yapıyı paylaşır (Grobauer vd., 2011). Çok sayıda kullanıcının aynı fiziksel kaynakları paylaşmasını sağlayan Çok Kiracılı Mimari (Multi-Tenancy), inceleme sırasında bir kiracının verilerine erişilirken diğer kiracıların gizliliğinin ihlal edilmemesi gerektiği anlamına gelir. Bu durum, her bir kiracının verisinin izole edilmesini ve güvenliğinin sağlanmasını gerektirir. Özellikle mahkemeye geçerli kanıt toplanırken etik ve hukuki açıdan dikkatli bir inceleme yapılmasını gerektirir (Emekci vd., 2016). Aşağıdaki örnek, bu mimarinin potansiyel risklerini göstermektedir.

Microsoft Azure Multi-Tenant Güvenlik Açığı (2021)

2021'de Microsoft Azure platformunda tespit edilen bir açık sayesinde bir kullanıcının, aynı fiziksel kaynakları paylaşan diğer kullanıcıların verilerine erişim sağlayabildiği ortaya çıktı. Güvenlik uzmanları bu durumu fark ettiklerinde Microsoft'a bildirdiler. Bu olay, çok kiracılı mimaride yeterli izolasyon sağlanmadığında büyük ölçekli veri ihlallerinin yaşanabileceğini göstermiştir (Aksakallı, 2019).

3.5. Veri Konumu, Egemenlik ve Yasal Sorumluluklar

Bulut ortamları çok uluslu hizmetler sunduğunda, veriler farklı ülkelerdeki veri merkezlerinde saklanabilir (Güngör, 2022). Bu durum, adli bilişim sürecinin yasal açıdan daha karmaşık hale gelmesine yol açar. Verilerin fiziksel olarak farklı ülkelerde depolanması, farklı yasal düzenlemelere tabi olmasını sağlar (bkz. Tablo 1). Bu da veri toplama ve erişim sırasında yasal engeller oluşturabilir. Bu da veri taleplerinde hukuki belirsizlikler yaratır (Tezcan, 2019).

Tablo 1. Bulut Hizmetlerinde Veri Lokasyonları ve Yasal Düzenlemeler Tablosu

Bulut Veri Depolama Ülkesi/Bölgesi	Örnek Cloud Bölgeleri	Yasal Düzenlemeler
Amerika Birleşik Devletleri (ABD)	AWS us-east-1, Azure US East, Google Cloud us-central1	CLOUD Act, HIPAA, COPPA, GLBA, CCPA/CPRA gibi eyalet yasaları
Avrupa Birliği (AB) Ülkeleri	AWS eu-west-1 (İrlanda), Azure West Europe (Hollanda), Google Cloud europe-west1 (Belçika)	GDPR, NIS2, Data Act, Data Governance Act, ulusal yasalar
Birleşik Krallık	AWS eu-west-2 (Londra), Azure UK South	UK GDPR, Data Protection Act 2018, Investigatory Powers Act 2016
Kanada	AWS ca-central-1 (Montreal), Azure Canada Central (Toronto)	PIPEDA, Quebec 25 Sayılı Yasası, Alberta & BC PIPA
Avustralya	AWS ap-southeast-2 (Sidney), Azure Australia East	Privacy Act 1988, SOCI Act, eyalet yasaları
Japonya	AWS ap-northeast-1 (Tokyo), Azure Japan East	APPI
Singapur	AWS ap-southeast-1, Azure Southeast Asia	PDPA, Cybersecurity Act
Brezilya	AWS sa-east-1 (São Paulo), Azure Brazil South	LGPD
Hindistan	AWS ap-south-1 (Mumbai), Azure Central India	DPDPA (2023)
Çin Halk Cumhuriyeti	AWS cn-north-1 (Pekin), Azure China North	CSL, DSL, PIPL

Microsoft İrlanda Davası (2013–2018)

ABD hükümeti FBI'ın talebi doğrultusunda uyuşturucu ticaretini konu alan bir soruşturmanın derinleştirilmesi için 2013 yılında Microsoft'tan, İrlanda'daki bir veri merkezinde saklanan e-posta verilerine erişim talebinde bulunmuştu. Microsoft, Elektronik İletişimin Gizliliği Hakkındaki Kanun'a göre verilerin İrlanda'da bulunması nedeniyle, ABD sınırları dışındaki verileri kapsayamayacağını bu nedenle talebin geçersiz olduğunu belirtti. Bu hukuki mücadele 2018'e kadar sürdü ve nihayetinde ABD'de çıkarılan CLOUD (Clarifying Lawful Overseas Use of Data) Yasası ile uluslararası veri taleplerinin önü açıldı (Amazon Web Services, t.y.). Merkez ofisleri Amerika Birleşik Devletleri'nde olsun ya da olmasın, ABD'de faaliyet gösteren tüm elektronik iletişim hizmeti sağlayıcıları ile uzaktan erişilebilen altyapı hizmeti sunan sağlayıcılar (örneğin e-posta ve CSP'ler), belirli düzenlemelere tabidir.

3.6. Türkiye'de Bulut Tabanlı Delillere Erişimde Yargı Yetkisi, Egemenlik ve Uluslararası İş Birliği

Bulut ortamlarında verilerin farklı ülkelerdeki veri merkezlerinde saklanabilmesi, adli bilişim sürecini yasal açıdan karmaşıklaştırır. Verilerin farklı ülkelerde bulunması, farklı yasal düzenlemelere tabi olmasına yol açar, bu da veri toplama ve erişimde yasal engeller ve hukuki belirsizlikler yaratabilir. Bu noktada uluslararası adli yardımlaşma mekanizmaları ve sözleşmeleri önem kazanır. Siber suçların sınır tanımayan doğası, devletler arası işbirliğini zorunlu kılar. Bu noktada, uluslararası adli yardımlaşma mekanizmaları ve sözleşmeleri önem kazanmaktadır (Tezcan, 2019).

Bu alandaki en önemli uluslararası düzenlemelerden biri, Avrupa Konseyi Siber Suçlar Sözleşmesi'dir (Council of Europe Convention on Cybercrime). Genellikle Budapeşte Sözleşmesi olarak da anılan bu sözleşme (European Treaty Series - ETS No. 185), siber suçlarla mücadelede uluslararası işbirliğini artırmayı ve taraf devletlerin ulusal yasalarını uyumlaştırmayı amaçlayan ilk bağlayıcı uluslararası antlaşmadır. Sözleşme, bilişim sistemlerine ve verilerine yönelik suçlar, bilgisayar bağlantılı sahtecilik ve dolandırıcılık, çocuk pornografisi ve telif hakları ihlalleri gibi geniş bir yelpazedeki suçları kapsamaktadır.

Ayrıca, sözleşme, elektronik delillerin toplanması ve sınır ötesi veri akışına ilişkin usul hükümleri de içermektedir; örneğin, bir ülkenin yetkili makamlarının, başka bir ülkenin topraklarında bulunan bir bilişim sistemindeki verilere erişimini kolaylaştıran maddeler içerir. Temel amaçları arasında, bilişim suçlarıyla ilgili ulusal yasal mevzuatları uyumlu hale getirmek, hızlı ve etkin bir uluslararası adli yardımlaşma ortamı oluşturmak ve siber suçlular için sığınma limanlarını yok etmek sayılabilir.

Türkiye, Avrupa Konseyi'nin kurucu üyelerinden biri olarak, Budapeşte Sözleşmesi'ni 10 Kasım 2010 tarihinde imzalamış ve sözleşme 29 Eylül 2014

tarihinde Türkiye açısından yürürlüğe girmiştir. Sözleşme, Türkiye'de "Sanal Ortamda İşlenen Suçlar Sözleşmesi" olarak resmi tercümesiyle bilinmektedir. (Tezcan, 2019).

Sözleşme, talep edilen tarafın, ricanın yerine getirilmesinin egemenliğine, güvenliğine, kamu düzenine veya diğer temel çıkarlarına zarar vereceğine inanması durumunda yardımı reddetme veya erteleme hakkını saklı tutar. Sözleşme'nin 15. Maddesi, öngörülen yetki ve usullerin, insan hak ve özgürlüklerinin korunmasını sağlayacak ve orantılılık ilkesini yerine getirecek şart ve güvencelere tabi olmasını şart koşar.

Budapeşte Sözleşmesi ve ek protokolleri (örneğin, sınır ötesi veri erişimini detaylandıran İkinci Ek Protokol), bulut bilişim ortamlarındaki adli süreçler için önemli bir yasal çerçeve sunsa da, uygulamada yasal süreçlerin işletilmesi, farklı ulusal yasalardaki farklılıklar ve teknolojik gelişmelerin hızı nedeniyle zaman alıcı ve karmaşık olabilmekte, sözleşme hükümlerinin tam uygulanmasında zorluklar yaşanabilmektedir.

4. CSP TARAFINDAN SAĞLANAN ADLİ İNCELEME SÜRECİNDE KULLANILAN TEKNİKLER VE ARAÇLAR

Adli bilişim süreci, dijital ortamlardaki olayların teknik analizini ve delillerin güvenli toplanarak hukuki süreçlerde kullanılabilir hale getirilmesini amaçlar. (Emekci vd., 2016). Bu süreç, genellikle aşağıdaki temel adımlardan oluşur: tespit, koruma, toplama, inceleme, analiz ve raporlama. Her aşamada farklı teknikler ve araçlar kullanılmaktadır.

CSP'ler tarafından sunulan araçlar, adli inceleme süreçlerini bazı açılardan kolaylaştırsa da, erişim seviyeleri ve veri formatları gibi konularda uzmanlar için yeni zorluklar da getirebilir.

4.1. Günlük Kaydı ve Olay İzleme Sistemleri

CSP'ler, kullanıcı ve sistem aktivitelerinin kaydedilmesini sağlayan log (günlük) yönetim sistemleri sunar. Log verileri, adli inceleme süreçlerinde zaman damgalarıyla birlikte şüpheli davranışların tespiti ve olayların kronolojik olarak yeniden inşası için hayati önem taşır. AWS CloudTrail, Azure Monitor ve Google Cloud Operations Suite (eski adıyla Stackdriver) gibi hizmetler bu kapsamda kullanılan araçlardandır.

4.2. Sanal Makine Anlık Görüntüleme ve Yedekleme

CSP'ler, VM'lerin anlık görüntülerini alma ve yedekleme hizmetleri sunarak delil niteliği taşıyabilecek verilerin bozulmadan saklanmasını sağlar (Quick vd., 2013). Snapshot alma işlemi, belirli bir anın sistem durumunu dondurarak daha sonra analiz

edilmesine olanak tanır. Snapshot'lar, adli analiz sürecinde; olay müdahalesi, veri kurtarma, yedekleme ve zararlı yazılımların analiz edilmesi için kullanılmaktadır. Google Compute Engine (GCE) Snapshots, Amazon EC2 Snapshots, Azure Virtual Machines Snapshots bu kapsamda kullanılmaktadır.

4.3. Uzaktan Adli Bilişim Erişimi

Canlı analiz, dijital adli incelemenin kritik bir aşamasıdır, çünkü verilerin ve sistemlerin değiştirilmeden ya da bozulmadan analiz edilmesi gerekir. CSP'ler, adli uzmanların, fiziksel erişimin mümkün olmadığı durumlarda bile uzaktan güvenli bir şekilde sistemlere ve verilere erişebilmesini sağlayacak araçlar ve Uygulama Programlama Arayüzleri (Application Programming Interface - API) sunar. Bu erişim yalnızca yetkilendirilmiş kişiler için açılır. AWS Systems Manager, Microsoft Azure Bastion bu hizmet kapsamında kullanılabilecek araçlara örnektir.

4.4. Şifreleme ve Bütünlük Doğrulama Araçları

Veri güvenliğini sağlamak için CSP'ler, veri şifreleme hizmetleri ve bütünlük doğrulama araçları sunar (Alenezi, 2021). Bu araçlar, delil toplama ve analiz aşamalarında veri bütünlüğünün korunmasına ve verilerin değiştirilip değiştirilmediğinin belirlenmesine yardımcı olur.

Bazı bulut sağlayıcılarının sunduğu hizmetler: AWS Key Management Service (KMS), Microsoft Azure Key Vault, Google Cloud Key Management Service (KMS).

4.5. Olay Müdahale ve Raporlama Araçları

CSP'ler, olay müdahale ekiplerinin tehditleri hızlı bir şekilde tespit etmelerini ve müdahale etmelerini sağlayacak araçlar sunar. Bu araçlar, şüpheli aktiviteleri analiz eder, olayları raporlar ve gerçek zamanlı olarak iletilir. Bazı bulut servis sağlayıcılarından örnekler; Amazon GuardDuty, Microsoft Azure platformunda Microsoft Defender for Cloud, Google Cloud da Security Command Center (SCC) hizmeti vardır (Aksakallı, 2019).

CSP'lerin sunduğu yerleşik araçların yanı sıra, üçüncü taraf güvenlik çözümleri de olay müdahale ve raporlama süreçlerinde önemli rol oynamaktadır. Bu üçüncü taraf araçlar, bulut güvenliği konusunda merkezi bir yönetim sunabilir ve birden fazla CSP platformunda sistemleri bulunan firmalar için entegre çözümler sağlayabilir.

5. VAKA ANALİZİ: LASTPASS OLAYI

Bu bölümde LastPass veri ihlali vakası incelenmektedir.

5.1. İlk Olay: Bulut Tabanlı Geliştirme Ortamındaki Erişim

Tarih: 8 Ağustos 2022 - 12 Ağustos 2022

Saldırı Vektörü: AWS, Access Keys, MFA,

İlk Olay Özet: LastPass güvenlik ekibi, bulut tabanlı geliştirme ortamında şüpheli faaliyetler fark etti ve incelemeye başladı. 13 Ağustos 2022'de olay müdahale süreçlerine destek olması amacıyla Mandiant ile anlaşma sağlamıştır. İncelemeler sonucunda; saldırgan, bir yazılım mühendisinin kurumsal dizüstü bilgisayarını ele geçirmiş ve bu cihazı kullanarak, aslında erişim izni olmayan kaynaklara sızmayı başarmıştır. Erişim sağlanan geliştirme ortamı, üretim verilerinden ayrılmıştı, bu nedenle müşteri verileri etkilenmemiştir.

Kritik Adımlar ve Alınan Aksiyonlar:

1. LastPass şüpheli aktiviteyi fark etti ve Mandiant ile anlaştı.
2. Saldırganın ilk vektörü, anti-forensik aktiviteler ve silinmiş sistem günlükleri nedeniyle tespit edilemedi.
3. Saldırgan VPN kullanarak kaynağını gizledi, mühendisin kimlik bilgilerini ve MFA'yı geçerek geliştirme ortamına erişti.
4. Erişim engellendi, cihazlar izole edildi, yetkiler yeniden yapılandırıldı. WAF kuralları güncellendi.
5. EDR çözümü güçlendirildi, VPN erişimi sıfır güven modeline dönüştürülmeye başlandı. Yeni CSPM platformu entegre edildi.
6. Çalınan kaynak kodları ve kimlik bilgileri güvence altına alındı, sertifikalar değiştirildi.

5.2. İkinci Olay: Saldırganın Geri Dönüşü

Tarih: 12 Ağustos 2022 - 26 Ekim 2022

Saldırı Vektörü: Anahtar dosyalarının ele geçirilmesi ve kötü amaçlı yazılımlar İlk İhbar: İlk saldırının ardından, saldırgan çalınan bilgileri, üçüncü bir tarafın veri ihlalinden elde ettiği bilgileri kullanarak ikinci bir saldırı başlattı. Bu bilgileri kullanarak bulut depolama alanına yeniden erişmeye çalıştı. Bu kez, bir DevOps mühendisinin şifreli yedeklemelere erişim sağlayabilmek için kişisel bilgisayarını hedef aldı. Keylogger kullanarak parolayı ele geçirdi.

Kritik Adımlar ve Alınan Aksiyonlar:

1. AWS GuardDuty şüpheli aktiviteyi tespit etti.
2. IAM rolleri sıkılaştırıldı, eski kullanıcılar devre dışı bırakıldı. Şifreleme anahtarları güvenli yönetildi, uzun vadeli anahtarların kullanımı engellendi.
3. Ev ve kurumsal ağ güvenliği, özellikle mühendislerin kişisel bilgisayarlarında güçlendirildi. MFA güçlendirildi (Microsoft PIN eşleştirmeli kimlik doğrulama).
4. DevOps mühendisinin bilgisayarındaki kötü amaçlı yazılımlar temizlendi.
5. Çalınan şifreli anahtarlar ve kritik sertifikalar sıfırlandı, IAM erişimleri yeniden yapılandırıldı. AWS S3 güvenliği artırıldı.

5.3. Sonuç ve İyileştirme Çalışmaları

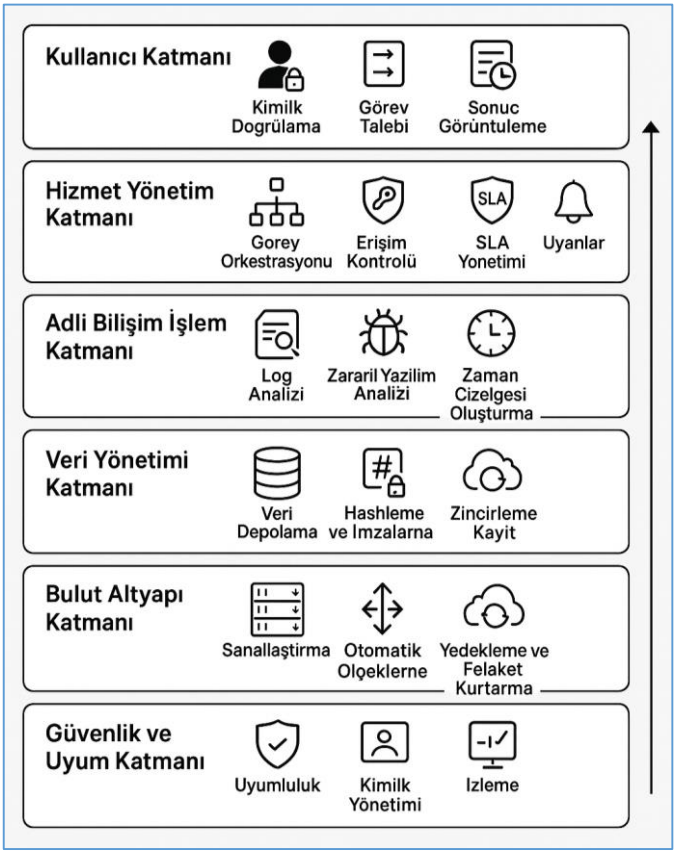
İkinci olayın ardından LastPass, üretim ortamlarında ek güvenlik kontrolleri başlattı ve bulut tabanlı altyapısındaki zayıf noktaları kapatmaya yönelik yeni stratejiler geliştirdi. Ayrıca, güvenlik izleme süreçleri daha da güçlendirildi, özellikle şüpheli aktiviteleri erkenden tespit etmek amacıyla ek güvenlik yazılımları entegre edildi. Olayın sonunda, tüm etkilenen geliştirme ortamları sıfırlandı ve yeniden yapılandırıldı (LastPass, 2023).

6. HİZMET OLARAK ADLİ BİLİŞİM (FORENSICS AS A SERVICE - FAAS)

Bulut bilişimin getirdiği zorluklar ve sunduğu imkanlar (önceki bölümlerde tartışıldığı gibi), adli bilişim süreçlerinin yürütülme biçiminde yeni yaklaşımların ortaya çıkmasına neden olmuştur. Bu bağlamda, literatürde bir süredir tartışılan ve geliştirilmekte olan Hizmet Olarak Adli Bilişim (Forensics as a Service - FaaS) modeli, dijital delil toplama, analiz etme ve raporlama süreçlerini bir hizmet olarak sunmayı amaçlamaktadır (Wen vd., 2013; Lee & Un, 2012).

FaaS modeli bulut adli bilişimi (cloud forensics) için önemli faydalar sunsa da, temel prensipleri ve yetenekleri sayesinde geleneksel digital forensics, ağ adli bilişimi (network forensics) gibi diğer adli bilişim dallarında da uygulanabilen bir yaklaşımdır. Temel amacı, adli bilişim süreçlerini daha verimli, hızlı ve erişilebilir kılmaktır (Kohn vd., 2013).

FaaS sistemleri genellikle modüler bir mimari üzerine kuruludur ve temel olarak şu bileşenleri ve işlevleri içerir (bkz. Şekil 2).



Şekil 2. FaaS Modelinin Temel Katmanları ve İşlevleri

(i) Uzak Kaynaklardan Delil Niteliği Taşıyan Verilerin Güvenli Biçimde Toplanması

FaaS'in ilk aşaması, dijital delillerin toplanmasıdır (Wen vd., 2013). FaaS, uzak kaynaklardan verilerin güvenli bir şekilde toplanmasını sağlar (Lee & Un, 2012). Bu süreç, veri kaybı veya bozulma riskini en aza indirir ve verilerin merkezi bir noktada saklanarak hızlı erişimini mümkün kılar. Örnek işlevler arasında log toplama (bkz. Şekil 3) ve ağ trafiği toplama (bkz. Şekil 4) bulunur.

FaaS İşlevi: collectLogs

Bu işlev, güvenlik cihazları veya sistemlerden log verilerini toplar ve bunları bulut ortamına yükler. Olayın tetiklenmesi ile otomatik olarak çalıştırılabilir.

```
const collectLogs = (logSource) => {
    let logs = fetchLogsFromSource(logSource);
    uploadToCloudStorage(logs);
};
```

Şekil 3. Log Toplama Fonksiyonu

FaaS İşlevi: collectNetworkTraffic

Ağ trafiği verilerini toplar, şüpheli veri transferlerini tespit etmek için kullanılır.

```
const collectNetworkTraffic = (networkSource) => {
    let networkData = fetchNetworkData(networkSource);
    uploadToCloudStorage(networkData);
};
```

Şekil 4. Ağ Trafiği Toplama Fonksiyonu

(ii) Veri Depolama ve Yönetimi (Secure Storage and Case Management)

Toplanan dijital delillerin güvenli, bütünlüğü korunmuş ve yasal gerekliliklere uygun bir şekilde (örneğin, farklı vakalar için izole edilmiş) depolandığı katmandır. Delil zincirinin (chain of custody) takibi bu katmanda sağlanır.

(iii) Verilerin Özel Adli Yazılımlar ve Büyük Veri Analiz Teknikleriyle İncelenmesi

FaaS'in ikinci işlevi, toplanan verilerin analiz edilmesidir. Bu aşamada, delil niteliği taşıyan veriler, özel adli yazılımlar ve büyük veri analiz teknikleriyle incelenir. FaaS sistemi bulut altyapısının gücünden yararlanarak çok büyük veri setlerini paralel işlemeyle hızlı bir şekilde analiz edebilir. FaaS, adli analizleri hızlı ve etkili şekilde gerçekleştirmek için ML ve AI gibi teknolojileri de kullanabilir. Bu sayede, şüpheli aktiviteler ve anormal durumlar otomatik olarak tespit edilebilir.

FaaS İşlevi: analyzeData (bkz. Şekil 5)

Toplanan verileri analiz eder, şüpheli aktiviteleri ve anormal durumları tespit eder.

```
const analyzeData = (logs, networkData) => {
    let anomalies = detectAnomalies(logs, networkData);
    if (anomalies) {
        triggerAlert(anomalies);
    }
};
```

Şekil 5. Analiz Fonksiyonu

FaaS İşlevi: runForensicAnalysis (bkz. Şekil 6) Adli yazılım ve analiz algoritmalarını çalıştırarak dijital delillerin kapsamlı analizini yapar.

```
const runForensicAnalysis = (evidenceData) => {
    let analysisResults = forensicSoftwareAnalyze(evidenceData);
    return analysisResults;
};
```

Şekil 6. Adli Analiz Algoritma Fonksiyonu

(iv) Analiz Sonuçlarının Yasal Süreçlere Uygun Biçimde Raporlanması

FaaS'in üçüncü temel işlevi, analiz sonuçlarının yasal süreçlere uygun bir şekilde raporlanmasıdır (Wen vd., 2013). Dijital delil toplama ve analiz işlemleri yalnızca teknik açıdan değil, aynı zamanda yasal açıdan da geçerli olmalıdır. FaaS, adli bilişim süreçlerinin yasal gereklilikleri karşılayacak şekilde yapılmasını sağlar (Lee & Un, 2012). Analiz sonuçları, dijital delillerin geçerliliği, güvenliği ve yasal uygunluğu göz önünde bulundurularak raporlanır. Raporlama aşamasında, bulut platformları sayesinde verilerin doğruluğu ve güvenliği sağlanabilir. Ayrıca, raporlar genellikle şeffaf ve denetlenebilir bir biçimde hazırlanır. Bu, hukuki süreçlerde kullanılacak dijital delillerin kabul edilebilirliğini artırır.

FaaS İşlevi: generateReport (bkz. Şekil 7)

Analiz sonuçlarını uygun şekilde raporlar.

```
const generateReport = (analysisResults) => {
    let report = createForensicReport(analysisResults);
    saveReportToDatabase(report);
    return report;
};
```

Şekil 7. Rapor Oluşturma Fonksiyonu

FaaS, genellikle üç farklı bulut modeli üzerinden sunulmaktadır: genel (public), özel (private) ve hibrit (hybrid) bulut (Furht & Escalante, 2010). Genel bulut FaaS hizmetleri, ölçeklenebilirlik ve düşük maliyet avantajı sağlarken; özel bulut çözümleri veri gizliliği açısından tercih edilmektedir. Hibrit yapılar ise esneklik ve denetim arasında bir denge kurar.

FaaS sistemlerinin yaygınlaşmasıyla birlikte, siber saldırıların veya sistem açıklarının neden olduğu olaylara hızlı müdahale edilebilmesi, olay yeri verilerinin bozulmadan korunması ve zamanla yarışan adli analizlerin daha verimli biçimde gerçekleştirilmesi mümkün hale gelmektedi. Ancak bu modelin uygulanmasında veri gizliliği, delil bütünlüğünün farklı yargı alanlarında sürdürülebilirliği, yasal yetki sınırları ve hizmet sağlayıcıya duyulan güven gibi önemli teknik, yasal ve etik zorluklar da göz önünde bulundurulmalıdır (Herman et al., 2014; Güngör, 2022).

7. BULUTTA KANIT YAŞAM DÖNGÜSÜ MODELİ (CELM) VE KANIT DEĞERLENDİRME SKALASI (KEBS)

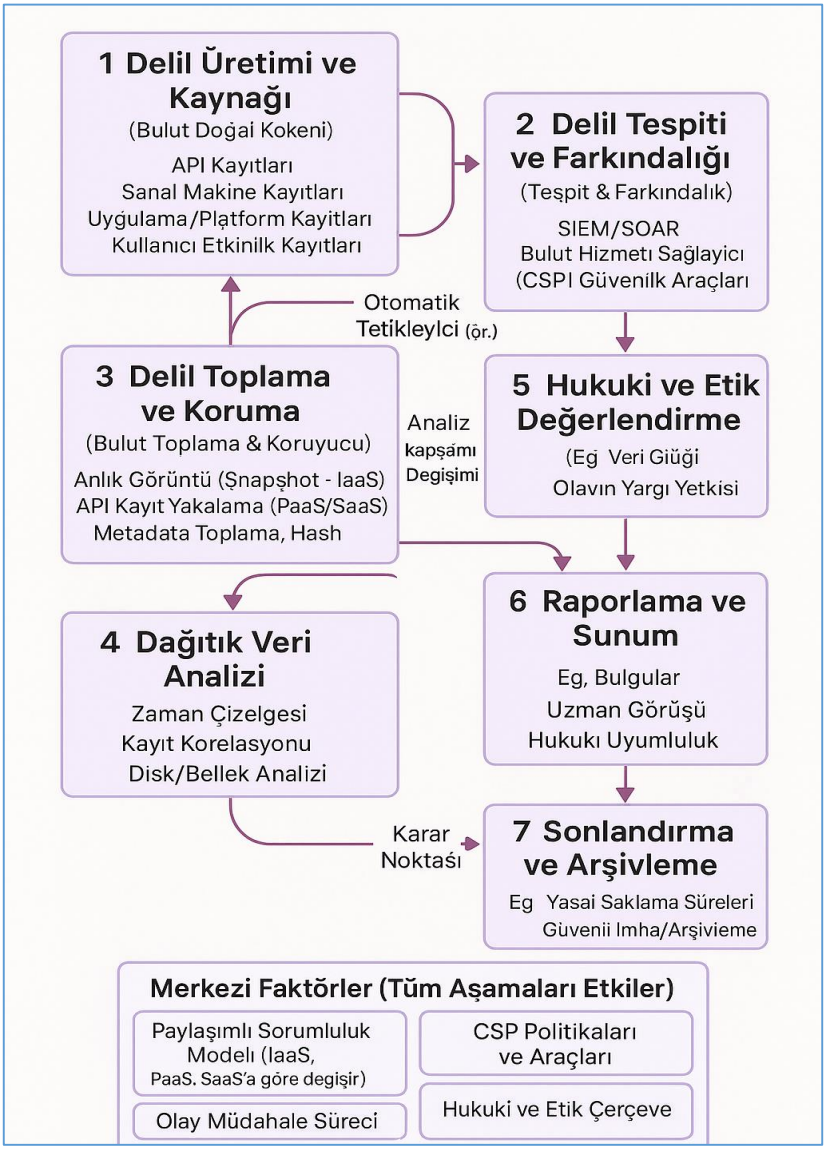
Bulut bilişim ortamlarının dinamik ve karmaşık yapısı, geleneksel adli bilişim yaklaşımlarının ötesinde, buluta özgü zorlukları ve fırsatları dikkate alan yeni modellere olan ihtiyacı ortaya koymaktadır.

Bu bölümde, bulut ortamında dijital kanıtın yaşam döngüsünü bütüncül bir perspektifle ele alan "Bulutta Kanıt Yaşam Döngüsü Modeli (CELM)" ve bu modelin aşamalarında elde edilen kanıtların kalitesini, güvenilirliğini ve kullanılabilirliğini değerlendirmek amacıyla geliştirilen "Kanıtın Erişilebilirlik ve Bütünlük Skalası (KEBS)" önerilmektedir. Bu özgün yaklaşımlar, "bulutta kanıt nerede başlar, nerede biter?" temel sorusuna metodolojik bir yanıt sunmayı, adli inceleme süreçlerine standart bir çerçeve getirmeyi ve kurumların proaktif adli hazırlık yeteneklerini geliştirmelerine katkıda bulunmayı amaçlamaktadır.

7.1. Bulutta Kanıt Yaşam Döngüsü Modeli (CELM)

CELM, dijital kanıtın bulut bilişim ortamında oluşumundan başlayarak, tespit edilmesi, toplanması, analiz edilmesi, yasal ve etik süzgeçlerden geçirilmesi, raporlanması ve nihayetinde yaşamının sonlanmasına (arşivlenme veya imha) kadar olan yedi temel aşamayı tanımlayan bir modeldir. Model, her bir aşamada bulutun kendine has özelliklerini (örneğin, sanallaştırma, kaynakların anlık dağıtımı, API tabanlı yönetim, paylaşılan sorumluluk, veri egemenliği vb.), IaaS, PaaS ve SaaS hizmet modelleri arasındaki farkları ve potansiyel otomasyon fırsatlarını dikkate alır.

CELM'in tüm aşamaları, Şekil 8'de gösterildiği gibi, "Merkezi Etkenler" olarak tanımlanan ve süreci sürekli etkileyen unsurlarla (Paylaşılan Sorumluluk Modeli, CSP Politikaları ve Araçları, Yasal ve Etik Çerçeve, Olay Müdahale Planı Entegrasyonu) çevrelenmiştir.



Şekil 8. Bulutta Kanıt Yaşam Döngüsü Modeli (CELM) ve Merkezi Etkenler

7.1.1. Aşama 1: Kanıt Oluşumu ve Kaynağı

Bu aşama, dijital kanıtın bulut ortamında ilk meydana geldiği anı ve bu kanıtın doğduğu kaynakları tanımlar. Geleneksel sistemlerdeki fiziksel cihazlardan farklı olarak, bulutta kanıt kaynakları genellikle sanal, dağıtık ve API tabanlıdır. Bu kaynakların türü ve erişim seviyesi, kullanılan bulut hizmet modeline (IaaS, PaaS, SaaS) ve Paylaşılan Sorumluluk Modeli'ne göre köklü değişiklikler gösterir:

IaaS (Altyapı olarak Hizmet): Kullanıcı geniş kontrole sahiptir. Kanıtlar; VM sistem logları, ağ akış logları, sanal disk imajları/snapshot'ları, kullanıcı güvenlik yazılımı logları ve CSP API çağrı logları (örn. AWS CloudTrail), IAM, Secrets Manager ve şifreleme anahtarı kullanım loglarıdır. Log detay seviyesi ve saklama süreleri proaktif planlanmalıdır.

PaaS (Platform olarak Hizmet): Kullanıcı, CSP tarafından yönetilen platformda uygulama geliştirir. Kanıtlar; kullanıcı uygulama logları, platform servis logları, platform API çağrı logları ve dağıtım/konfigürasyon kayıtlarıdır. Altyapı loglarına erişim genelde sınırlıdır.

SaaS (Yazılım olarak Hizmet): Kullanıcı kontrolü en azdır. Kanıtlar; SaaS uygulamasının denetim (audit) logları, kullanıcı aktivite kayıtları, yönetici eylem logları ve uygulama güvenlik uyarılarıdır. Erişim, uygulama arayüzü veya sınırlı API'lerledir. Kurumların loglama ve veri saklama yetenekleri, bu aşamada kanıtın detayını ve erişilebilirliğini etkiler.

Bu aşamada, kurumların farklı işletme ölçeklerine göre değişen loglama ve veri saklama yetenekleri, kanıtın oluşumundaki detay seviyesini ve daha sonraki aşamalardaki erişilebilirliğini doğrudan etkiler.

7.1.2. Aşama 2: Kanıt Tespiti ve Farkındalık

Bu aşama, potansiyel bir güvenlik olayının, bir anormallik veya adli inceleme gerektirecek şüpheli bir aktivitenin varlığının ilk fark edildiği noktadır. Tespit, çeşitli yöntemlerle gerçekleşebilir:

Otomatik Tespit Sistemleri: CSP güvenlik servisleri (örn. AWS GuardDuty), SIEM, SOAR, IDS/IPS, WAF logları ve özel alarmlar.

Manuel Tespit Süreçleri: Sistem yöneticilerinin, güvenlik analistlerinin veya son kullanıcıların rutin kontrolleri, sistem performansındaki beklenmedik değişiklikler veya şüpheli bir e-posta/davranışla karşılaşmaları sonucu olayı fark etmeleri.

Üçüncü Taraf Bildirimleri: Müşterilerden, iş ortaklarından, dış güvenlik araştırmacılarından veya kolluk kuvvetlerinden gelen ihbarlar.

Bu aşamada, olayın ciddiyeti ve potansiyel kapsamı hakkında bir ön değerlendirme yapılır ve KEBS (bkz. Bölüm 7.2) açısından potansiyel kanıt kaynaklarının erişilebilirlik ve bütünlük durumları hakkında ilk tahminler yürütülmeye başlanabilir.

7.1.3. Aşama 3: Kanıt Toplama ve Güvence Altına Alma

Tespit edilen olayla ilgili dijital delillerin, delil bütünlüğünü koruyarak ve yasalara uygun bir şekilde toplanması, kopyalanması ve güvenli bir şekilde saklanması bu aşamanın temelini oluşturur. Bulut ortamında toplama yöntemleri, fiziksel erişimin

olmaması nedeniyle geleneksel yöntemlerden önemli ölçüde farklılaşır ve CSP araçlarına/API'lerine bağımlıdır.

Eksik/Toplanamayan Veri Durumu: Teknik, yasal veya sözleşmesel nedenlerle verilere ulaşılamayabilir; bu durumlar ve etkileri belgelenmelidir.

Tamamen Erişim Kaybı Riski: Hesap ele geçirilmesi veya CSP kaynaklı kesintiler gibi durumlara karşı harici yedekleme ve multi-region stratejileri değerlendirilir.

Yedekleme ve Multi-Region Stratejileri: Kanıtın alternatif kopyalarının farklı coğrafi bölgelerde bulunması erişilebilirliği ve bütünlüğü artırır.

Delil Bütünlüğü ve Zinciri: Toplanan delillerin hash değerleri hesaplanır, delil zinciri titizlikle belgelenir. Her bir kanıt için KEBS ile detaylı erişilebilirlik ve bütünlük değerlendirmesi yapılır.

Bu aşamada, her bir toplanan kanıt için KEBS (bkz. Bölüm 7.2) kullanılarak detaylı bir erişilebilirlik ve bütünlük değerlendirmesi yapılır.

7.1.4. Aşama 4: Kanıt Analizi ve Korelasyon

Bu aşamada, toplanan ham veriler işlenir, anlamlı bilgilere dönüştürülür, olayların yeniden canlandırılması sağlanır ve farklı kaynaklardan (IaaS, PaaS, SaaS; farklı log türleri; farklı zaman dilimleri) gelen kanıtlar birbiriyle ilişkilendirilerek olayın bütüncül bir resmi oluşturulur.

Analiz Ortamı: Güvenli bir laboratuvarda özel adli bilişim yazılımları veya güvenliği sağlanmış bulut tabanlı analitik platformlar kullanılır.

Temel Analiz Teknikleri: Zaman çizelgesi analizi, log korelasyonu, disk/bellek imajı analizi, ağ trafiği analizi.

KEBS Etkisi: Analiz sırasında, KEBS puanı yüksek kanıtlara genellikle daha fazla ağırlık verilir. Düşük KEBS puanına sahip kanıtlar dikkatle ve diğer kanıtlarla çapraz doğrulama yapılarak değerlendirilir. Eksik veya toplanamayan verilerin analize etkisi bu aşamada netleştirilir.

7.1.5. Aşama 5: Kanıtın Yasal ve Etik Değerlendirmesi

Toplanan kanıtların ve uygulanan adli bilişim yöntemlerinin yerel ve uluslararası yasalara (örneğin, KVKK, CMK, GDPR), endüstri standartlarına ve etik ilkelere uygunluğu kapsamlı bir şekilde değerlendirilir.

Değerlendirme Kriterleri:

- Veri gizliliği ve mahremiyeti.
- Yargı yetkisi ve veri egemenliği.
- CSP ile yapılan sözleşmeler (SLA'lar).

- Uluslararası anlaşmalar (örn. Budapeşte Sözleşmesi).
- Delil kabul edilebilirliği.
- CSP işbirliği düzeyi. KEBS'in "Yasal ve Sözleşmesel Erişilebilirlik (E-YS)" ve "Erişim Kaybı Riski (E-EKR)" faktörleri bu aşamada önemlidir.

7.1.6. Aşama 6: Kanıt Raporlama ve Sunum

Tüm analiz sonuçlarının, elde edilen kanıtların, kullanılan yöntemlerin, KEBS değerlendirmelerinin ve uzman görüşlerinin ilgili taraflara açık, anlaşılır, objektif, tarafsız ve yasal gerekliliklere uygun bir şekilde raporlanmasıdır.

Rapor İçeriği Özetle:

- Olay özeti, inceleme kapsamı, deliller ve KEBS skorları, analiz yöntemleri, bulgular, sonuçlar, uzman görüşü ve öneriler.
- Eksik/toplanamayan verilerin analize etkisi net bir şekilde açıklanmalıdır.
- Delil zinciri ve hash doğrulama adımları detaylandırılmalıdır. "Alınan Dersler ve İyileştirme Önerileri Raporu", kurumun gelecekteki olaylara karşı direncini artırmak için Proaktif Adli Hazırlık Geri Besleme Döngüsü'nü besler.

7.1.7. Aşama 7: Kanıtın Yaşam Sonu ve Arşivleme

Adli inceleme ve ilgili yasal süreçler tamamlandıktan sonra, toplanan dijital delillerin ve vaka dosyalarının yasal saklama sürelerine ve kurum politikalarına uygun olarak güvenli bir şekilde uzun süreli arşivlenmesi veya usulüne uygun olarak imha edilmesi aşamasıdır.

Arşivleme: Delillerin bütünlüğü korunarak (şifreli, hash'li olarak) uzun süreli saklama için uygun maliyetli ve güvenli depolama çözümleri kullanılır. Arşivlenmiş verilere erişim prosedürleri tanımlanmalıdır.

İmha: Artık gerekmeyen veya yasal saklama süresi dolmuş verilerin bulut ortamından ve diğer depolama alanlarından güvenli ve geri döndürülemez bir şekilde silinmesi. CSP'lerin veri silme mekanizmalarının ve garantilerinin anlaşılması önemlidir.

7.2. Kanıtın Erişilebilirlik ve Bütünlük Skalası (KEBS)

KEBS, CELM'in özellikle "Kanıt Toplama ve Güvence Altına Alma" ve "Kanıt Analizi ve Korelasyon" aşamalarında, her bir dijital kanıtın adli bilişim açısından güvenilirliğini ve kullanılabilirliğini dinamik ve yapılandırılmış bir şekilde değerlendirmek için önerilen bir puanlama sistemidir. Temel amacı, adli bilişim

uzmanına kanıtın kalitesi hakkında objektif bir görüş sunmak, soruşturmanın güçlü ve zayıf yönlerini belirlemek ve kaynakların etkin kullanımını sağlamaktır.

7.2.1. KEBS Sınıflandırma Faktörleri

KEBS, kanıtı iki ana boyut altında ve bu boyutları etkileyen çeşitli alt faktörler üzerinden değerlendirir:

Tablo 2. KEBS Erişilebilirlik (E) ve Bütünlük (B) Sınıflandırma Faktörleri

Boyut	Faktör Kodu	Faktör Adı	Değerlendirme Kriterleri (1: Çok Kötü - 5: Çok Yüksek)
ERİŞİLEBİLİRLİK (E)	E-DT	Veri Kaynağının Doğrudanlığı ve Teknik Erişilebilirlik	Kanıta teknik erişimin kolaylığı/zorluğu, API/araç gereksinimi, veri formatı.
	E-VTK	Veri Toplama Durumu ve Kapsamı	Kanıt kaynağında eksik/toplanamayan veri oranı ve bunun erişime etkisi.
	E-YS	Yasal ve Sözleşmesel Erişilebilirlik	Yasal engeller, veri egemenliği, SLA kısıtları, CSP işbirliği düzeyi.
	E-ŞA	Şifreleme ve Anahtar Yönetimi	Veri şifreliyse anahtara erişim kolaylığı ve etkinliği.
	E-YCY	Yedekleme ve Coğrafi Yedeklilik	Güvenilir ve erişilebilir yedeklerin varlığı, multi-region/multi-AZ stratejisi.
	E-EKR	Erişim Kaybı Riski ve Önlemler	Kanıt kaynağına erişimin tamamen kaybolma riski ve bu riske karşı alınan önlemlerin etkinliği.
	E-MZ	Maliyet ve Zaman Faktörü	Veriye erişim/toplama maliyeti ve süresinin makuliyeti.
BÜTÜNLÜK (B)	B-KD	Kriptografik Doğrulama	Hash doğrulaması, dijital imzalar.
	B-DZ	Delil Zinciri (Chain of Custody)	Kanıtın her aşamasının detaylı, kesintisiz ve güvenilir belgelenmesi.
	B-DM	Verinin Değişmezliği	Logların/verilerin üzerine yazılma, silinme, değiştirilme riskinin düşüklüğü
	B-KG	Kaynak Güvenilirliği ve Tutarlılığı	Verinin kaynağının bilinirliği, güvenilirliği, farklı kopyalar/zamanlar arasındaki tutarlılık.
	B-YK	Yedeklerin ve Kopyaların Bütünlüğü	Yedeklerin alınırken, saklanırken ve geri yüklenirken bütünlüğünün korunması ve doğrulanması.
	B-VTK	Veri Toplama Durumunun Bütünlüğe Etkisi	Eksik veya toplanamayan verinin, mevcut verilerin genel bütünlüğünü ve anlamını ne ölçüde etkilediği.

7.2.2. KEBS Puan Hesaplama ve Yorumlama

Her bir alt faktör (E-DT, B-KD vb.) için, yukarıdaki tablo ve işletmenin özel durumu dikkate alınarak 1 (Çok Kötü) ile 5 (Çok İyi) arasında bir puan atanır.

Adım 1: Ana Boyut Puanlarının Hesaplanması (E ve B Puanları)

Her ana boyut (Erişilebilirlik ve Bütünlük) için, alt faktör puanlarının ağırlıklı ortalaması alınır. Ağırlıklar, adli bilişim uzmanının veya kurumun her bir alt faktöre atfettiği öneme göre belirlenebilir (Örneğin, B-KD %35, B-DZ %25 gibi). Standart bir başlangıç için eşit ağırlık da kullanılabilir, ancak hassas bir değerlendirme için ağırlıklandırma önerilir. (bkz. Denklem 1, Denklem 2)

$$E = \frac{\sum(E_i \cdot w_i)}{\sum w_i}$$

Denklem 1. Erişilebilirlik Puanının Değerlendirme Formülü

- E : Genel E Puanı (1-5)
- Ei : Alt Faktör E puanı
- wi : Ağırlık

$$B = \frac{\sum(B_i \cdot w_i)}{\sum w_i}$$

Denklem 2. Bütünlük Puanının Değerlendirme Formülü

- B : Genel B Puanı (1-5)
- Bi : Alt Faktör B puanı
- wi : Ağırlık

Adım 2: KEBS Kategorisinin Belirlenmesi

Elde edilen E ve B puanları, aşağıdaki gibi bir matris kullanılarak kanıtın genel güvenilirlik ve kullanılabilirlik kategorisini belirlemek için kullanılır:

Tablo 3. KEBS Güvenilirlik ve Kullanılabilirlik Matrisi

BÜTÜNLÜK (B) → ERİŞİLEBİLİRLİK (E) ↓	1 (Çok Düşük)	2 (Düşük)	3 (Orta)	4 (Yüksek)	5 (Çok Yüksek)
1 (Çok Düşük)	Kullanılamaz	Çok Düşük	Çok Düşük	Düşük	Düşük
2 (Düşük)	Çok Düşük	Düşük	Düşük	Orta	Orta
3 (Orta)	Çok Düşük	Düşük	Orta	Orta	Yüksek
4 (Yüksek)	Düşük	Orta	Orta	Yüksek	Yüksek
5 (Çok Yüksek)	Düşük	Orta	Yüksek	Yüksek	Çok Yüksek

Bu matris, her bir kanıt parçası için "Çok Yüksek", "Yüksek", "Orta", "Düşük", "Çok Düşük" veya "Kullanılamaz" gibi bir güvenilirlik/kullanılabilirlik kategorisi atar. Bu kategori, kanıtın adli incelemedeki ağırlığını, rapordaki sunumunu ve mahkemede kabul edilebilirliğini etkileyebilir.

7.3. Proaktif Adli Hazırlık Geri Besleme Döngüsü

Bu döngü, her CELM uygulamasından (adli incelemeden) ve KEBS değerlendirmesinden elde edilen "Alınan Dersler"in, kurumun bulut ortamındaki genel adli hazırlık seviyesini ve gelecekteki kanıtların KEBS skorlarını sürekli olarak iyileştirmek için kullanılmasını amaçlar. Bu, reaktif bir yaklaşımdan proaktif ve sürekli öğrenen bir adli hazırlık kültürüne geçişi ifade eder.

7.3.1. Döngünün İşleyişi

CELM Uygulaması ve KEBS Değerlendirmesi: Bir olay incelenir, CELM aşamaları takip edilir ve ilgili kanıtlar için KEBS değerlendirmesi yapılır.

"Alınan Dersler" Raporu ve İyileştirme Önerileri: CELM'in "Raporlama" aşamasının bir çıktısı olarak, inceleme sürecindeki başarılar, zorluklar (özellikle KEBS puanı düşük çıkan kanıtlar ve nedenleri), eksiklikler ve iyileştirme fırsatları detaylı bir şekilde belgelenir.

Proaktif Aksiyonların Planlanması ve Uygulanması: Bu rapordaki öneriler (örneğin, loglama politikalarının güncellenmesi, IAM yetkilerinin sıkılaştırılması, yedekleme stratejilerinin iyileştirilmesi, SLA'ların gözden geçirilmesi, CSP araçlarının daha etkin kullanımı, çalışan eğitimleri) somut aksiyon planlarına dönüştürülür ve uygulanır.

Hazırlık Seviyesinin Artırılması: Uygulanan bu aksiyonlar, kurumun genel siber dayanıklılığını ve bir sonraki potansiyel olay için adli hazırlık seviyesini yükseltir.

Bu, CELM'in "Hazırlık" (örtük olarak ilk aşaması) ve "Kanıt Oluşumu" aşamalarını doğrudan etkiler.

7.3.2. Proaktif Adli Hazırlık Checklist'i (Örnek)

Aşağıdaki checklist, "Alınan Dersler" sürecini yapılandırmak ve iyileştirme alanlarını belirlemek için kullanılabilir. Her madde, farklı işletme ölçekleri için özelleştirilebilir ve KEBS bulgularıyla ilişkilendirilebilir.

Tablo 4. Proaktif Adli Hazırlık Geri Besleme Döngüsü Ana Başlıkları

Kontrol Alanı	Değerlendirme Soruları	Önerilen İyileştirme Aksiyonu
1. Loglama ve İzleme	Saklama süreleri ve detay seviyeleri uygun muydu? Loglar merkezi ve değişmez miydi?	Loglama politikalarının güncellenmesi, yeni log kaynaklarının eklenmesi, saklama sürelerinin artırılması,
2. Kimlik ve Erişim Yönetimi (IAM)	En az yetki prensibi uygulanıyor muydu? MFA etkin miydi?	MFA'nın zorunlu kılınması, düzenli IAM denetimleri.
3. Sır Yönetimi (Secrets Management)	Hassas sırlar güvenli yönetiliyor muydu?	Merkezi sır yönetim aracına geçiş, sır rotasyon politikaları, erişim loglarının takibi.
4. Veri Yedekleme ve Kurtarma / Multi-Region	Yedekleme politikaları yeterli miydi? Multi-region stratejisi var mıydı, etkin miydi?	Yedekleme sıklığının/kapsamının artırılması, değişmez yedekler, multi-region yapılandırması,
5. Kanıt Toplama ve Saklama Prosedürleri	Snapshot alma, log indirme, hash hesaplama süreçleri tanımlı ve etkin miydi? Eksik/toplanamayan veri veya erişim kaybı riski nasıl yönetildi?	Otomatik delil toplama script'lerinin geliştirilmesi, harici güvenli depolama, CSP ile SLA'ların ve iletişim protokollerinin güncellenmesi.
6. Güvenlik Araçları	CSP güvenlik araçları (GuardDuty vb.) etkin miydi?	Araçlarının yapılandırmasının optimizasyonu, yeni araçların değerlendirilmesi.
7. Olay Müdahale Planı ve Tatbikatlar	Olay müdahale planı bu tür bir bulut olayı için güncel ve yeterli miydi?	Olay müdahale planının buluta özgü senaryolarla güncellenmesi
8. Personel Farkındalığı ve Eğitimi	Çalışanlar yeterli bilgiye sahip miydi?	Düzenli güvenlik farkındalık eğitimleri.

8. ÖNERİLER

Bulut tabanlı sistemlerin artan kullanımı, adli bilişim süreçlerinin teknik ve organizasyonel olarak yeniden yapılandırılmasını gerekli kılmaktadır. Bu doğrultuda, bulut hizmeti kullanıcıları ve adli inceleme uzmanlarının olay müdahale süreçlerini iyileştirip güvenlik ihlallerine karşı daha hazırlıklı olmalarına yardımcı olabilecek öneriler şunlardır:

8.1. Adli Müdahale Senaryoları ve Tatbikatlar

Kurumlar, bulut ortamında gerçekleşebilecek siber olaylara karşı özel olarak hazırlanmış adli müdahale senaryoları oluşturmalıdır. Breach & Attack Simulation ekipleri ve sızma testi (pentest) ekipleri, bulut ortamlarına özel olarak geliştirilen tehdit senaryolarını kullanarak hem altyapının hem de güvenlik politikalarının dayanıklılığını test etmelidir. Bu testler, örneğin IAM yanlış yapılandırmaları, veri sızıntıları veya hatalı loglama gibi zafiyetleri önceden tespit etmede oldukça etkilidir. Saldırı simülasyon ürünleri de sürekli test ve tehdit doğrulama imkânı sunarak önleyici tedbirlerin geliştirilmesine katkı sağlar.

Bu tatbikatların planlanmasında CELM aşamaları, elde edilen bulguların (toplanabilen/toplanamayan kanıtlar vb.) değerlendirilmesinde ise KEBS bir rehber olabilir. Tatbikatlardan elde edilen dersler, CELM'in 'Proaktif Adli Hazırlık Geri Besleme Döngüsü' ve 'Proaktif Adli Hazırlık Checklist'i' ile kurumsal süreçlere entegre edilmelidir.

Tatbikatlar sadece teknik personelle sınırlı kalmamalı, hukuk, yönetim ve veri sorumluluğu taşıyan birimler de (hem kullanıcı kurumda hem de adli süreçlerde) sürece entegre edilmelidir.

8.2. Uyumluluk ve Güvenlik Politikaları

Kurumlar, kullandıkları sistemlerin yerel ve uluslararası regülasyonlara (örneğin GDPR, KVKK, HIPAA) uyumunu düzenli olarak denetlemelidir. CSP'lerin veri merkezi konumları dikkatle seçilmeli ve verilerin yasal açıdan uygun, kuruma en yakın merkezde tutulması hedeflenmelidir.

CSP sözleşmelerinde verilerin depolanacağı bölge, aktarım koşulları ve adli inceleme taleplerine yanıt prosedürleri açıkça belirtilmelidir. Güvenlik ve uyumluluk politikalarının oluşturulması ve denetlenmesinde, CELM'in 'Kanıt Oluşumu ve Kaynağı' ile 'Yasal ve Etik Değerlendirme' aşamaları; loglama ve veri saklama politikalarının etkinliğinin değerlendirilmesinde ise KEBS'in 'Erişilebilirlik' boyutu kritik öneme sahiptir.

8.3. Eğitim ve Farkındalık

Hem bulut hizmeti kullanan kurum çalışanlarına hem de adli bilişim uzmanlarına yönelik sürekli veri güvenliği ve bulut bilişim eğitimleri düzenlenmelidir. Bu eğitimlerde, CELM'in tüm aşamaları ve KEBS değerlendirme faktörleri hakkında bilgi verilerek buluta özgü tehditler ve kanıt toplama süreçleri konusunda farkındalık artırılmalıdır.

Sistem yöneticileri, güvenlik uzmanları ve analistler, buluta özgü tehditler, delil toplama yöntemleri ve savunma mekanizmaları hakkında yetkin olmalıdır.

8.4. Şeffaflık ve İzlenebilirlik

Kurumlar (bulut kullanıcıları), hizmet aldıkları CSP'lerin loglama, denetim ve raporlama olanaklarını iyi analiz etmeli; mümkünse gelişmiş izleme araçları kullanmalıdır. Adli bilişim uzmanları için, olayların zaman çizelgesi çıkarılabilir şekilde, bütüncül ve ayrıştırılabilir log kayıtları talep edilmeli ve bu logların formatı, içeriği ve saklama süreleri hakkında net bilgi sahibi olunmalıdır.

8.5. Güncelleme

Hazırlanan güvenlik ve olay müdahale planları, teknolojik gelişmelere ve yeni tehditlere karşı (hem kullanıcı kurumlar hem de adli bilişim birimleri tarafından) düzenli olarak güncellenmelidir (Grobauer vd., 2011).

Yeni hizmet alınan veya altyapısı değiştirilen CSP'ler için ayrı denetim ve adaptasyon süreçleri işletilmelidir.

8.6. Olay Müdahale Süreçlerinin Otomatize Edilmesi

Özellikle adli bilişim uzmanları için, uçucu verilerin hızlı kaybı nedeniyle, olay anında sistemden otomatik olarak veri (kritik loglar, anlık bellek dökümleri vb.) çekecek ve güvenli şekilde saklayacak script'ler ve otomasyon araçları geliştirilmeli veya kullanılmalıdır (bkz.6)

9. SONUÇLAR VE DEĞERLENDİRMELER

Bulut ortamları, dijital dönüşümle birlikte veri depolama, işleme ve erişim süreçlerini önemli ölçüde dönüştürmüştür. Ancak bu dönüşüm, geleneksel adli bilişim süreçleri için dinamik yapı, fiziksel erişim sınırlamaları ve veri konumu sorunları gibi büyük zorluklar da ortaya çıkarmaktadır. Bu zorluklar, doğru teknikler, araçlar ve titiz bir hukuki-etik yaklaşımla aşılabilir. LastPass vakası, bulut güvenliğinde kurumsal önlemlerin yanı sıra Bulut Hizmet Sağlayıcısı (CSP) çözümlerinin etkin kullanımı ve bireysel kullanıcı farkındalığının da kritik olduğunu göstermiştir.

Makalenin temel sorusu olan "Bulut ortamında kanıt nerede başlar, nerede biter?" sorusunun yanıtı, geleneksel sistemlere kıyasla çok daha katmanlı ve değişkendir.

Kanıtın Başlangıç Noktası: Çoğu zaman olayın ilk tespit edildiği an ve ilgili ilk dijital izdir (örneğin, bir log kaydı, API çağrı kaydı, CSP güvenlik servisinden bir alarm, bir sanal makine anlık görüntüsü). LastPass vakasındaki AWS GuardDuty alarmları ve ilk şüpheli faaliyetlerin tespiti bu duruma örnektir. Geleneksel sistemlerdeki fiziksel imaj almanın yerini bulutta genellikle VM anlık görüntüsü veya log toplama alır.

Kanıtın Bitiş Noktası: Bu nokta çok daha karmaşık ve değişkendir; yalnızca teknik sınırlara (veri uçuculuğu, şifreleme, anti-forensik teknikler) değil, aynı zamanda yasal erişim yetkilerine (veri egemenliği, uluslararası yasal süreçler), etik ilkelere, hizmet sözleşmelerine (SLA) ve CSP ile işbirliği düzeyine de bağlıdır. LastPass vakasında saldırganın ilk vektörünün logların silinmesi nedeniyle tespit edilememesi veya Microsoft Ireland davasındaki yargı yetkisi sorunları bu sınırları örneklendirir. Ayrıca, paylaşılan sorumluluk modeline (IaaS, PaaS, SaaS) göre CSP'nin ve müşterinin erişebileceği veri katmanları farklılık gösterir.

Geleneksel adli bilişimdeki fiziksel sınırlar bulut ortamında bulanıklaşmış, delilin kapsamı ve erişilebilirliği daha dinamik ve çok boyutlu hale gelmiştir. Bu nedenle, bulut adli incelemesinde "kanıtın sonu", genellikle teknik, yasal ve operasyonel kısıtların kesişim noktasında, her vaka özelinde farklılaşarak belirlenir ve hem teknik araçlara hakimiyet hem de yasal prosedürlere dair çok yönlü bir değerlendirme gerektirir. Bu çalışma, bulutta kanıtın başlangıç ve bitiş noktalarını mevcut zorluklar, CSP araçları, FaaS gibi yaklaşımlar ve LastPass gibi güncel bir vaka analizi üzerinden bütüncül bir şekilde değerlendirmenin yanı sıra, bu dinamik sınırları netleştirmek ve adli inceleme süreçlerine standart bir yaklaşım getirmek üzere özgün Bulutta Kanıt Yaşam Döngüsü Modeli (CELM) ve Kanıtın Erişilebilirlik ve Bütünlük Skalası (KEBS) modellerini önererek literatüre katkı sağlamaktadır.

KAYNAKÇA

6698 sayılı Kişisel Verilerin Korunması Kanunu. (2016). Resmi Gazete, 29677, 1–6.

Alenezi, M. (2021). Safeguarding cloud computing infrastructure: A security analysis. Computer Systems Science and Engineering, 37(2), 159–167.

Al Sadi, Ghania. "Cloud computing architecture and forensic investigation challenges. " International Journal of Computer Applications 124.7 (2015).

Big Data Bilişim. (2025). Bulut depolama alanlarının adli incelenmesi. https://bigdata.com.tr

Cloud Act. (n.d.). https://aws.amazon.com/tr/compliance/cloud-act/

Digital Forensics as a Service: A game changer - Scientific Figure on ResearchGate. (2025, May 9). https://www.researchgate.net/figure/IDFPM-Digital-forensic-investigation-Kohn-etal-2013_fig2_261762759

Emekci, A., Kuğu, E., & Temiztürk, M. (2016). Adli bilişim ezberlerini bozan bir düzlem: Bulut bilişim. UBGMD, 2(1), 8–14. https://doi.org/10.18640/ubgmd.08216

Emekci, Ş., Güray, E., & Kılınç, A. (2016). Bulut bilişim ortamlarında adli bilişim uygulamaları. Uluslararası Bilgisayar ve Bilgi Teknolojileri Sempozyumu. Dergipark.org.tr

Furht, B., & Escalante, A. (2010). Handbook of cloud computing. Springer Publishing Company.

Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. IEEE Security & Privacy, 9(2), 50–57.

Grispos, G., Glisson, W. B., & Storer, T. (2014). Using cloud computing to achieve organizational security goals.

Güngör, E. (2022). Yargı yetkisi sorunları bağlamında bulut bilişim sistemleri ve adli delil elde etme. Bilişim Hukuku Dergisi. Dergipark.org.tr

Herman, M., Iorga, M., Halterman, R., & NIST Cloud Computing Forensic Science Working Group. (2014). Cloud computing forensic science challenges (NISTIR 8006). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/ir/8006/final

Kişisel Verileri Koruma Kurumu. (2018). Kişisel verilerin korunması kanununa ilişkin uygulama rehberi (ss. 56–61). KVKK Yayınları.

LastPass (2023, Mart 1). Security incident update and recommended actions. https://blog.lastpass.com/posts/security-incident-update-recommended-actions

Lee, J., & Un, S. (2012, October). Digital forensics as a service: A case study of forensic indexed search. In 2012 International Conference on ICT Convergence (ICTC) (pp. 499–503). IEEE.

Ministry of Electronics and Information Technology (MeitY). (2023). The Digital Personal Data Protection Act, 2023 (DPDPA). Government of India. https://www.meity.gov.in/data-protection-framework

National Institute of Standards and Technology. (2014). Cloud computing forensic science challenges (NISTIR 8006). U.S. Department of Commerce. https://csrc.nist.gov/pubs/ir/8006/final

Nourmandi-pour, R., & Vosoogh, A. (2015). Scheduling problems for cloud computing. Cumhuriyet Üniversitesi Fen Edebiyat Fakültesi Fen Bilimleri Dergisi, 36(3), 2628–2652.

Parmar, V. N., Rana, U. D., & Vaghela, R. (2024). Review on challenges in cloud forensics. International Journal of Science and Research (IJSR), 13(6), 113–118. https://doi.org/10.21275/SR24531104809

Peterson, G., & Shenoi, S. (Eds.). (2013). Impact of cloud computing on digital forensic investigations. In Advances in Digital Forensics IX (Vol. 410, pp. 291–303). Springer.

Quick, D., Martini, B., & Choo, R. (2012). Cloud storage forensics (pp. 1–12). Elsevier.

Reilly, D., Moyne, J. T., & Abidin, A. (2013, May). Cloud forensics issues and opportunities. Paper presented at the Information Technology and Communications Conference (ITACC), Ireland.

Rehberg, R. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review, 50, 105840. https://doi.org/10.1016/j.clsr.2023.105840

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud forensics: An overview. In Digital Forensics and Cyber Crime (Vol. 361, pp. 35–47). Springer.

Seeba, M., Valgre, M., & Matulevičius, R. (2025). Evaluating organization security: User stories of European Union NIS2 Directive. arXiv. https://arxiv.org/abs/2504.19222

Tezcan, D. (2019). Bilişim suçlarında uluslararası adli yardımlaşma. Yaşar Hukuk Dergisi, 1(2), 287–294.

Wen, Y., Man, X., Le, K., & Shi, W. (2013). Forensics-as-a-service (FaaS): Computer forensic workflow management and processing using cloud. In The Fifth International Conferences on Pervasive Patterns and Applications (pp. 1–7). IARIA.

Srinivasan, A., & Ferrese, F. (2019). Forensics-as-a-Service (FaaS) in the state-of-the-art cloud. L. Chen, H. Takabi, & N.-A. Le-Khac (Ed.), Security, privacy, and digital forensics in the cloud (ss. 321-337). Wiley-IEEE Press. https://doi.org/10.1002/9781119053385.ch16

Zawoad, S., & Hasan, R. (2015). Cloud forensics: A meta-study of challenges, approaches, and open problems. IEEE Transactions on Services Computing, 8(3), 420-430.