KİŞİSEL VERİLER ve SİBER GÜVENLİKTE ORTAK BÜYÜK TEHLİKE: VERİTABANLARINDA ULUSAL STRATEJİ NE OLMALI?

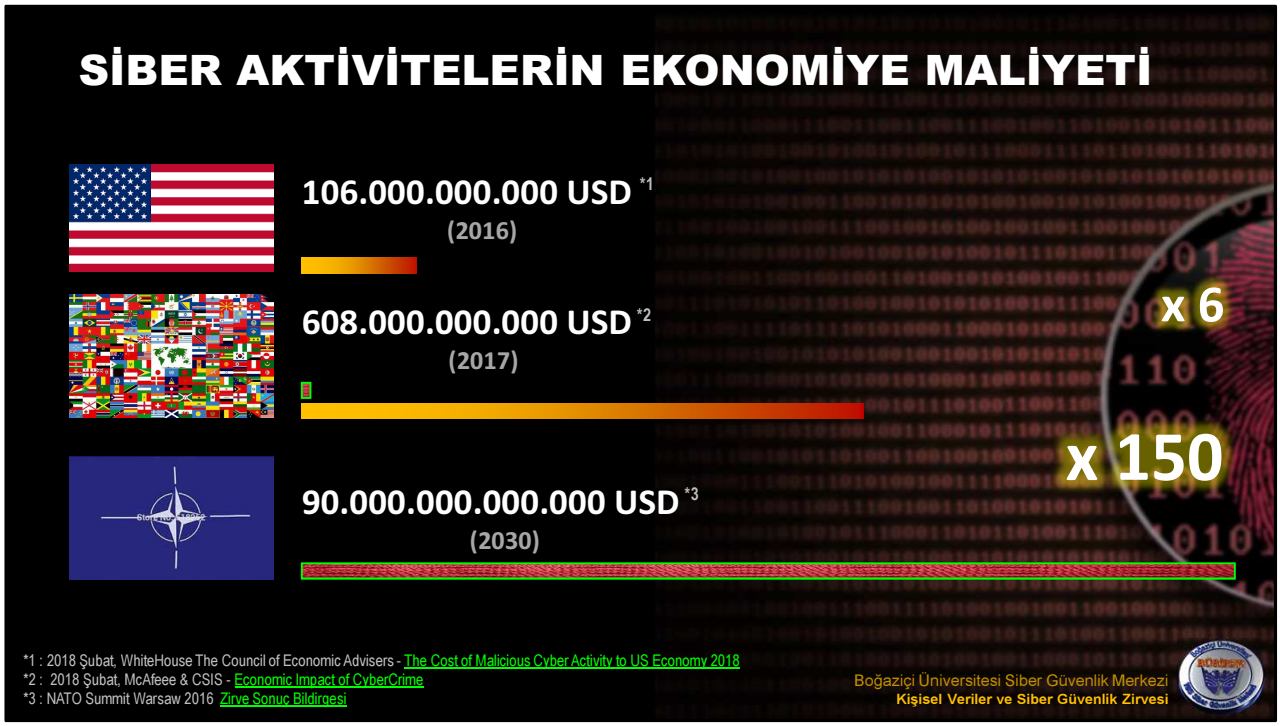
Mustafa AFYONLUOĞLU

Bu sunum, 01 Mart 2018 tarihinde, Boğaziçi Üniversitesi Siber Güvenlik Merkezi (BÜSİBER) tarafından gerçekleştirilen «Kişisel Veriler ve Siber Güvenlik Zirvesi 2018» de gerçekleştirilmiştir.

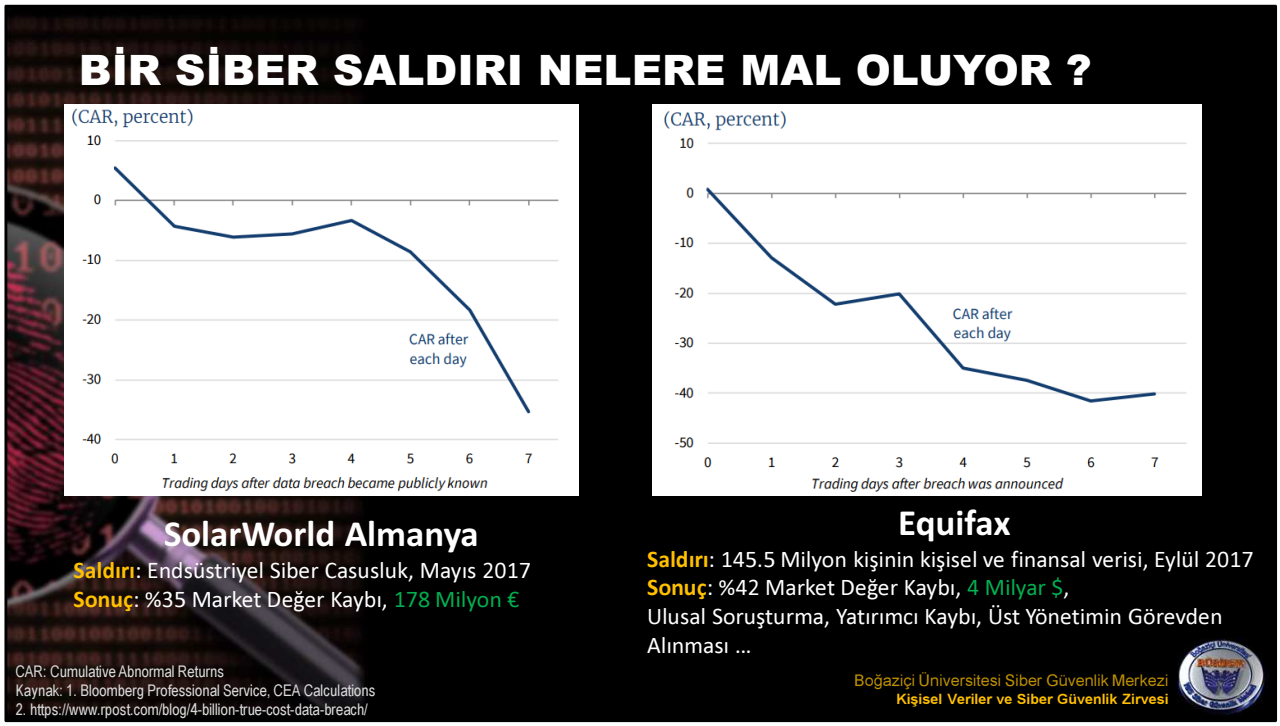
Sunumda, siber güvenlik bakımından korumak durumunda olduğumuz verinin ve özellikle kişisel verilerin muhafaza edildiği ve yönetildiği «veri tabanları»nda bizleri bekleyen riskler ve bunlara karşı alınması gereken tedbirleri içeren bir ulusal yol haritası ele alınmaktadır. Bu sunumda öne sürülen çözümlere esas olarak 30 (otuz) tane iyi bilinen ve yaygın kullanılan Açık Kaynak Kodlu (AKK) veritabanı çözümü incelenmiştir. Bu çözümlere ilişkin detaylı kıyaslama tablolarının yer aldığı inceleme çalışması ayrıca:

http://afyonluoglu.org/millilik-hedefleri-siber-guvenlik-kisisel-veriler-ucgeninde-milli-veri-tabani/

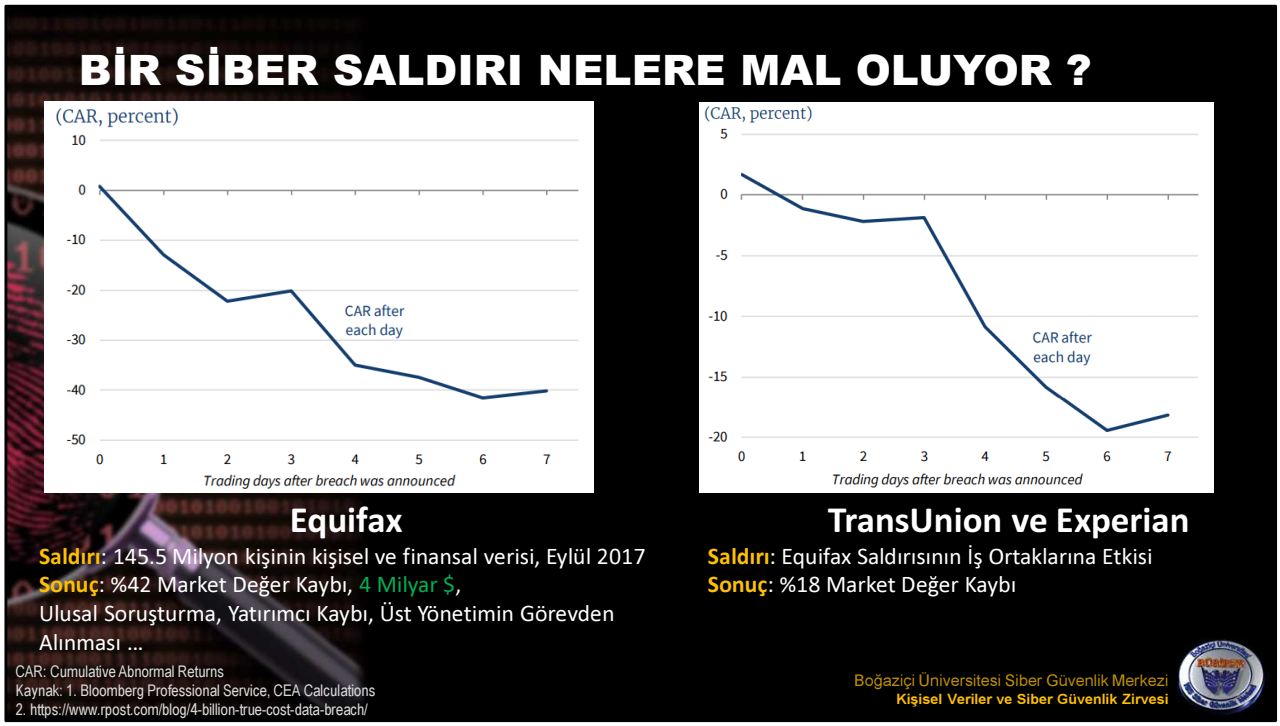
adresinde yayınlanmıştır.



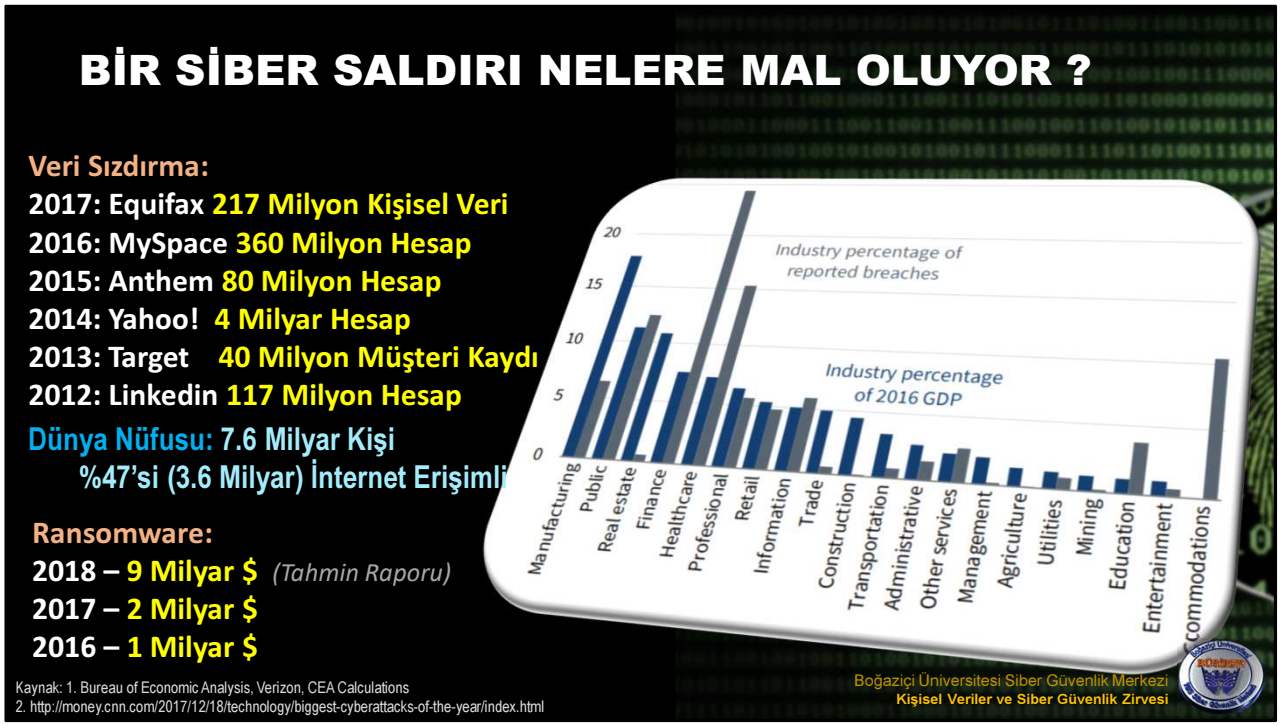
Şubat 2018'de yayınlana iki temel raporda siber saldırıların ülke ve dünya ekonomilerine maliyeti ele alınmıştır. Beyaz Saray Ekonomik Danışma Konseyi tarafından yayınlanan «Zararlı Siber Aktivitelerin Amerika Ekonomisine Maliyeti 2018» başlıklı raporda, ABD'nin 2016 yılında siber aktivitelerin 106 Milyar Dolara mal olduğu vurgulanmaktadır. McAfee ve CSIS tarafından yayınlanan «Siber Suçun Ekonomik Etkisi 2018» Raporu'nda ise dünyaya maliyetin 608 Milyar Dolara ulaşmakta olduğu belirtilmiştir. NATO, 2016 Varşova Zirvesi'nde, Denver Üniversitesi'ne yaptırdığı bir araştırma sonucunu açıklamış ve 2030 yılında Siber Güvensizliğin dünyaya maliyetinin 90 Trilyon Dolara ulaşacağı açıklanmıştır.



Özel sektör bakımından da siber saldırılar oldukça yıkıcı olmaktadır. Son altı aylık dönem incelendiğinde büyük markaların siber saldırılar sonucu market değerlerini %40 seviyesinde kaybettiği görülmektedir. Örneğin Mayıs 2017 tarihinde endüstriyel siber casusluğa uğrayan Almanya merkezli SolarWorld, saldırıdan sonra ilk 7 gün içerisinde %35 market değer kaybına uğramıştır. Eylül 2017'de 145.5 milyon kişinin kişisel verileri ile finansal bilgilerinin sızdırıldığı Equifax olayında ise saldırının duyulmasından sonraki bir hafta içerisinde %42 market değer kaybı yaşanmış, ayrıca ulusal soruşturma açılmış ve yatırımcıların uzaklaştığı görülmüş, olay ayrıca üst yönetimin görevden alınmasına sebep olmuştur.

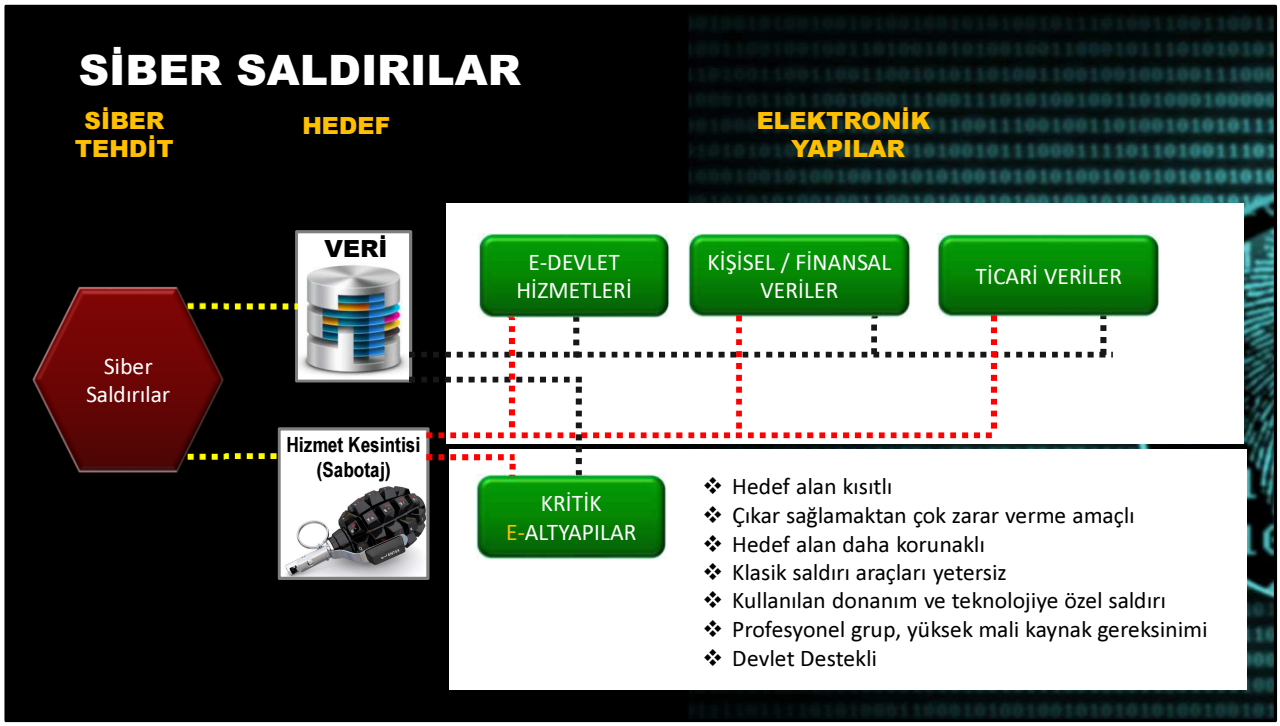


Siber saldırılar ayrıca, saldırıya uğrayan özel sektörün çözüm otağı olan şirketleri de ağır şekilde etkilemektedir. Örneğin Equifax olayında, doğrudan siber saldırıya uğramadığı ve herhangi bir bilgi ve veri kaybına sebep olmadığı halde, Equifax'ın çözüm ortağı olan TransUnion %18 market değer kaybına uğramıştır.



Siber saldırıların sonuçlarının bu kadar yıkıcı ve yüksek maliyetli olmasının sebebi, ele geçirilen verilerin çok yüksek sayılarda olmasıdır. Son 5-6 yıla baktığımızda artık 100 milyonlarca kişiye ait verinin ele geçirilmesine artık alışmakta olduğumuzu görüyoruz. Hatta son dönemde birkaç milyar kişiye ait verinin ele geçirildiğine şahit olduk. Eküm 2017 verilerine göre dünya nüfusunun 7.6 Milyar kişi olduğu ve bu nüfusun yaklaşık %47'sinin internete eriştiğini dikkate alırsak, günümüz itibarı ile siber saldırılar neticesinde neredeyse dünya üzerindeki herkesin kişisel ve/veya finansal verileri sızdırılmış durumdadır. Üstelik rapor edilen veri sızıntıları incelendiğinde neredeyse tüm sektörlerde bu sızıntıların yaşandığı görülmektedir. Elbette beklendiği üzere üretim, finans ve konaklama gibi sektörlerde bu sızıntının seviyesi diğerlerine göre çok daha yüksektir.

Bir diğer siber maliyet ise fidye yazılımlardan gelmektedir. 2015 yılında yarım milyar dolar rapor edilen fidye seviyesi sonraki yıl ikiye ve peşindeki yıl olan 2017'de tekrar ikiye katlanmış olup içinde bulunduğumuz yıl için ise neredeyse 5'e katlanarak 9-10 milyar dolar seviyesinde fidyeye ulaşacağı tahmin edilmektedir.



Bu yüksek kayıplar açısından siber saldırıları incelediğimizde 2 temel hedef olduğunu görmekteyiz:

1. Verileri Ele Geçirme: Burada elde edilmek istenen veriler kamuya ait e-devlet hizmetleri çerçevesinde üretilen belge ve bilgiler, kamu ve sektördeki kişisel ve finansal veriler ile sektördeki ticari veriler ve sırlardır.
2. Hizmet Kesintisi ve Sabotaj: Daha çok kritik altyapılara uygulanan bu saldırı biçimi daha kısıtlı bir hedef alanına sahiptir. Bu saldırılar çıkar sağlamaktan çok zarar verme amaçlıdır ve saldırılmaya çalışılan altyapı (enerji, ulaşım, sağlık gibi) işin niteliği itibarı ile daha korunaklı olduğundan klasik saldırı araçları yetersiz kalmakta ve saldırılacak yerde kullanılan donanımlara özelleştirilmiş yöntem ve teknolojilerin kullanılmasını zorunlu tutmaktadır. Bu sebeple bu tür saldırılar profesyonel gruplar aracılığıyla yapılmakta ve zaten state-sponsored dediğimiz devlet destekli olarak yürütülmektedir. Dolayısıyla bu alan daha özel olarak ele alınması gerektiğinden, bu sunumda daha çok verilerin ele geçirilmesi yoluyla ortaya çıkan riskler ve çözüm önerileri ele alınmıştır.

Devlet verileri, kişisel veriler, finansal veriler ve ticari veriler gibi başlıklarda karşılaşılabilecek siber saldırılara karşı en iyi tedbir, «**üreticisinin aklıyla**» hareket etmeyen «**sadık**» çözümlerden geçmektedir. Yani, bu alanlarda kullanılan çözümler, «sadece» başta açıkça belirtilen ve taahhüt edilen fonksiyonlara ilişkin hizmet vermeli, «başka» arka-kapı faaliyetlerine yeltenmemelidir.

Bu açıdan bakıldığında «**veriyi üreten**» teknoloji olarak «**yazılım**»da **MİLLİ** çözümlerin kullanılmasına ilişkin yeterince farkındalık oluşmuş ve hatta bu konuda gerek yazılımsal gerekse donanımsal milli çözümler son aylarda ardı ardına basın yoluyla duyurulmaya başlanmış, bunların da olumlu sonuçları hızla alınmaya başlanmıştır.

Ancak bu ekosistemde gözden kaçan önemli bir husus, bu yazılımların ürettiği «**veriyi depolayan ve yöneten**» veritabanlarıdır. Bu veritabanlarına bakıldığında, korumak istediğimiz kişisel veriler, finansal bilgiler, devlet belgeleri dahil tüm verilerimizin burada muhafaza edildiğini görmekteyiz. Dolayısıyla «veriyi korumak» istiyorsak, hem yazılım hem de veritabanına bir bütün olarak bakmak zorundayız. Bu sebeple **veritabanı** da **MİLLİ** olmak zorundadır.

Milli Veritabanı'nı hayata geçirmek için şu adımlar önerilmektedir:

1. Öncelikle, tekerleği baştan keşfetmemek ve günümüze kadar gelmiş deneyimlerden faydalanmak için, temel alınacak veritabanı teknolojisi belirlenmelidir. Çözümün her kademesine hakim olmak için, incelenecek adaylar herşeyden önce **açık kaynak kodlu** olmalıdır. Ayrıca hizmet verecek kesim incelendiğinde birbirleriyle kıyaslanamayacak çeşitlilikte hacimler göze çarpmaktadır. Örneğin bir kurumun bir yılda ürettiği belge sayısı 300.000 iken bir başka kurumun sadec bir GÜNDE ürettiği belge sayış 3.8 milyondur. Dolayısıyla ortaya konulacak çözüm hem **ölçeklenebilir** olmalı, hem de **yüksek performans** sergilemeli, ayrıca bütünlüğü ve birlikte çalışabilirliği en üst seviyede sağlayabilmek için **standartlara tam uyum** sağlanmalıdır.

Bu arada en kritik ön şart **TAM MİLLİLİK**'tir. Yani aday çözüm tüm alt bileşenleri de dahil olmak üzere hiçbir KARA KUTU içermemeli, yani tamamının kaynak kodları erişilebilir ve kullanılabilir olmalıdır.

Aday çözümde önemli olan bir diğer husus **kitle-kaynak kullanım** ile geliştirmeye uygun olmasıdır. Ülkemizde, açık kaynak kodlu çözümle başlamış ancak kapalı olarak geliştirildiği için dünyadaki glişmelere yetişememiş ve başarısız olmuş çalışma örnekleri mevcuttur. Aynı başarısızlığa tekrar düşmemek için aday çözüm bileşenler

halinde ve üniversiteler ve açık topluluklar gibi farklı kitlelerle de geliştirmeye açık olmalıdır.

Ayrıca bu veritabanı çözümü çok farklı bilgi seviyelerinde çok farklı ekipler tarafından kullanılacağından, kendisini en iyi şekilde anlatan detaylı bir **dokümantasyon**a sahip olmak zorundadır.

Ayrıca çözümün güncel kalması için halihazırda **yaygın bir kesim tarafından kullanılıyor olması**, **büyük hacimli çözümler** tarafından tercih edilmiş olması da önemli bir seçim kriteridir.

Bu kriterler açısından ele alındığında, incelenen 30 açık kaynak kodlu çözüm arasında en uygun çözümün POSTGRESQL olduğu görülmektedir.

Bu çözümlere ilişkin detaylı kıyaslama tablolarının yer aldığı
inceleme çalışması ayrıca:

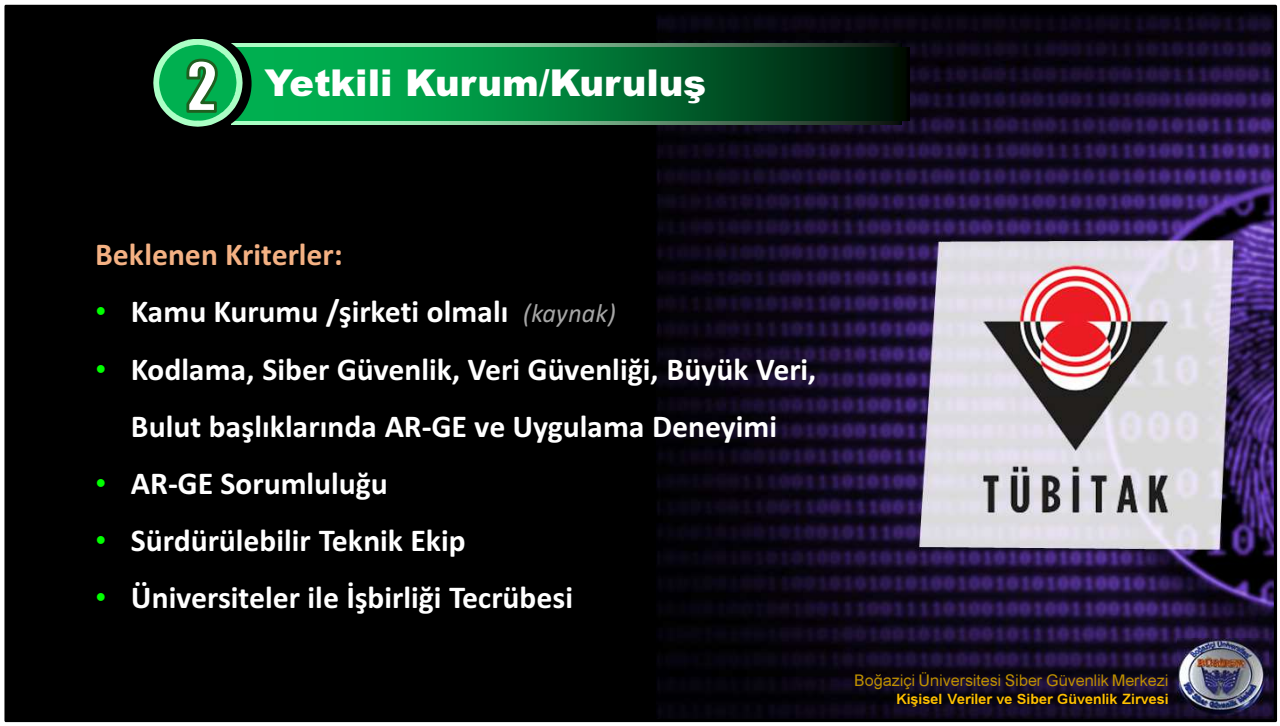
http://afyonluoglu.org/millilik-hedefleri-siber-guvenlik-kisisel-veriler-ucgeninde-milli-veri-tabani/

adresinde yayınlanmıştır. İncelenen çözümlerin 2018 yılı itibarı ile halen aktif olmaları, tercihen mevcut yapıları itibarı ile 2017 yılında ödül almış ya da referans gösterilmiş olmaları dikkate alınmıştır. İnceleme analizi ayrıca aşağıdaki başlıkları içermektedir:

- İşletim Sistemleri ve Platformlar ile uyumluluk
- Avantajları
- Dezavantajları
- Referans büyük kullanıcılar / platformlar
- Erişilebilirlik (Web Sitesi, Geliştirme Platformları, Çözüm Forumları vb.)

İncelenen 30 çözümden 18 tanesi SQL tabanlı standart veritabanı çözümleridir.

Ayrıca belge tabanlı ve CBS gibi çözümler için grafik tabanlı veritabanları ve platformlar da incelenmiştir.



2. Milli Veri tabanı sürecindeki ikinci aşama, bu ürün konusundaki yetkili kurum/kuruluşun belirlenmesidir. Her ne kadar açık kaynak kodlu mevcut bir veri tabanı çözümü esas alınacak olsa da, milli veri tabanı çalışması aslen AR-GE niteliğindedir. Yani sürekli geliştirilmeye ve üzerinde araştırma yapılmaya muhtaçtır. Bu da sürekli ve düzenli bir kaynak (hem insan kaynağı hem de mali kaynak) gerektirir. Bu sebeple, ulusal bailıklarda ihtiyaç duyulan AR-GE açlışmalarının kamu kurumu marifetiyle yapılması prensibi ile, bu konudaki yetkili kurumun bir kamu kurumu olması en uygun seçenek olacaktır.

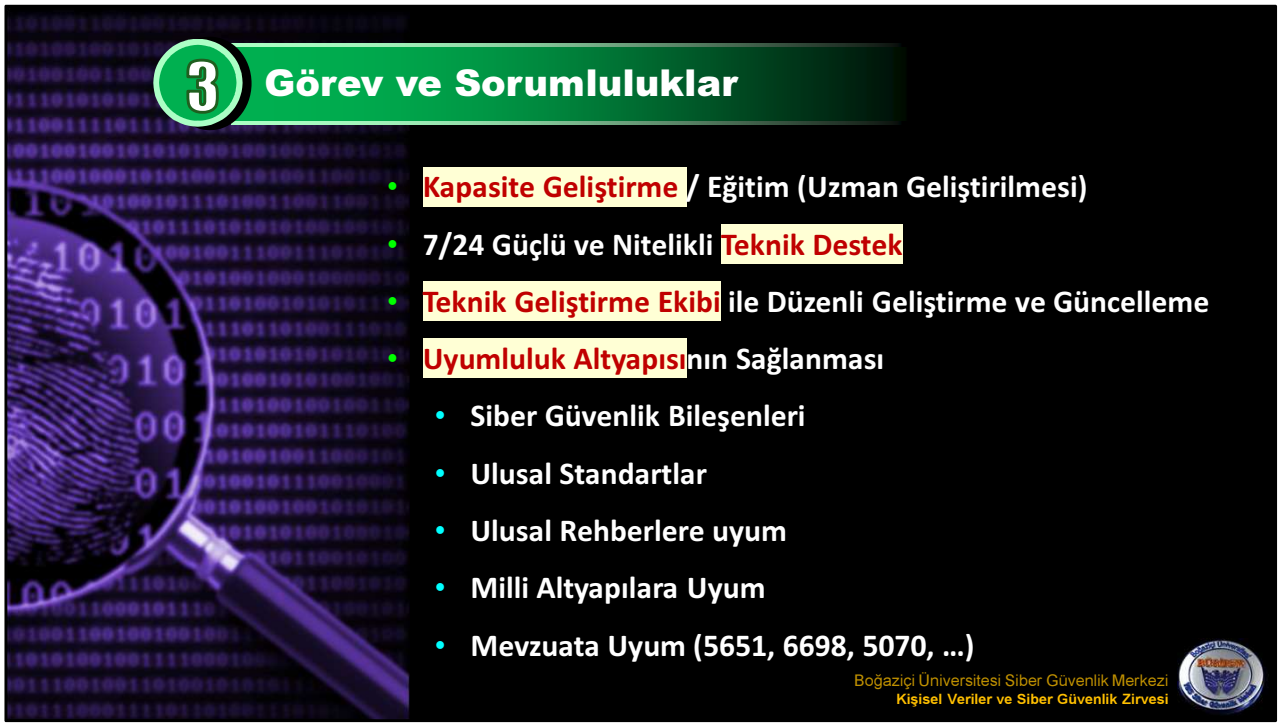
Bu kamu kurumunda aranması gereken temel nitelikler ele alınacak olursa:

a) Veri tabanı ile doğrudan ilişkili olan teknolojiler bakımından bu kurumun siber güvenlik, veri güvenliği, büyük veri ve bulut başlıklarında AR-GE ve uygulama deneyimi olmalı, ayrıca yazılım kodlama konusunda pratik deneyimi olmalı ve belirli uluslararası standartlar ve çerçevelere uyum göstermelidir.
b) Kurumun asli sorumluluğu AR-GE olmalı, katma değer yaratma ve araştırma yapma kabiliyeti ve deneyimi yüksek olmalıdır.
c) Sürdürülebilir bir yapı ihtiyacına binaen, kurum bünyesinde bu amaçla yer alan sürekliliği sağlanmış bir teknik ekip yer almalıdır. Kurum bu ekibi oluştururken çatısı altındaki diğer birimlerden, üniversitelerden ve diğer kamu kurumlarından

süreli veya sürekli tecrübeli insan kaynağını istihdam etme imkanına sahip olmalıdır. Teknik ekibin sirkülasyon yaşamaması ve milli veri tabanı başlığında kurumsal hafızanın korunması esas olmalıdır.

d) Veri tabanı başlığında üniversitelerde de ciddi bir deneyim ve ileriye yönelik araştırma çalışmaları yer almaktadır. Dolayısıyla üniversitelerde bu başlıkta işbirliği yapmak mutlaka şartır. Bu bağlamda, kurumun üniversiteler ile işbirliğinde geniş bir tecrübesi olması, bu ekosistem ile uyumlu çalışma ortamının oluşturulması bakımından önemli bir kriterdir.

Tüm bu kriterler esas alındığında, (muhakkak ki başka alternatifler de mevcuttur), öncelikli olarak AR-GE yükümlülüğü, siber güvenlik, yazılım ve bahsedilen diğer alanlardaki farklı enstitülerinde oluşmuş tecrübesi bakımından TÜBİTAK, milli veri tabanı yetkili kurumu olarak güçlü bir seçenektir.



3. Belirlenen yetkili kurumdan beklenen görev ve sorumlulukların ortaya konulması, sürecin üçüncü önemli adımıdır:

a) Günümüzde maalesef bir çok kamu kurumunda teknik birikime sahip uzmanları istihdam etmek veya bu kişilerin sürekliliğini sağlamak zor olmakta, veri tabanı gibi daha nitelkli alanlar söz konusu olduğunda bunun sağlanması daha da güçleşmektedir. Nitekim bu sebeptendir ki, kamu kurumları veri tabanı seçimlerinde, ürünün niteliklerinden çok iki temel kriteri esas almaktadır:
   - Ürüne 7/24 verilecek teknik destek ile, herhangi bir anda ortaya çıkan sorunlara anında çözüm sağlanması ve böylece kurum sorumluluğundaki elektronik hizmetlerde hiçbir aksama yaşanmaması
   - Ürünün ihtiyacın daha üzerinde bir kapasitede olması, böylece yazılım geliştirme sürecinde de yaşanan benzer insan kaynağı problemlerinden kaynaklı kötü kodlamanın getireceği olumsuz yüklerin hizmete yansımaması, veri tabanının her halükarda (kötü tasarlanmış yazılım kodlaması çalışsa dahi) yüksek performansta hizmet vermesi

Her iki yaklaşım da sonuç olarak ülke ekonomisine ilave maliyetler olarak geri dönmektedir. Bunu önlemenin tek yolu nitelikli insan kaynağının oluşturulması (kapasite geliştirme) ve akabinde bu ekiplere iyileştirilmiş özlük haklarının

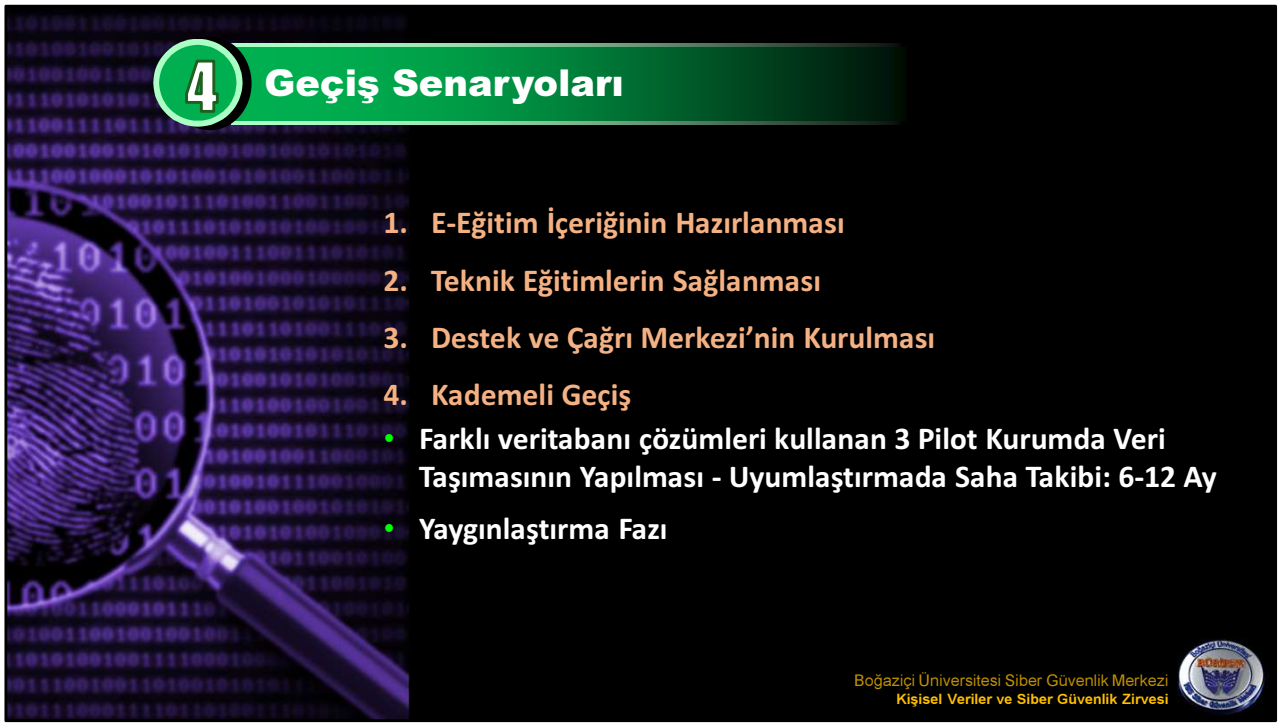
sunulmasıdır. Bu çerçevede, mevcut milli veri tabanı için de, kurumlarda kapasite oluşturmaya ilişkin bir eğitim altyapısı hazırlanması, yetkili kurumun görev ve sorumluluğunda olacaktır.

b) İlk maddede anlatılan gerekçeler çerçevesinde, yetkili kurum, tüm kamu kurum ve kuruluşlarına, (verilen elektronik hizmetlerde kesinti yaşanmaması amacıyla) 7/24 destek verebilecek ekipler oluşturmalıdır. Bu ekipler klasik Çağrı Merkezi anlayışından öte, teknik olarak ürüne ve problem çözümlerine hakim nitelikli teknik kişilerden oluşmalıdır.

c) Yetkili kurum tarafından oluşturulacak teknik ekip ile, milli veri tabanı çözümü sürekli geliştirilecek, güncel ihtiyaçların otaya koyacağı yeni kütüphaneler hazırlanacak ve testleri gerçekleştirilerek dağıtımı sağlanacaktır.

d) Milli veri tabanı geleneksel veri tabanı hizmetlerini sunmanın ötesinde belirli ulusal uyumlulukları da doğal olarak içermelidir. Bu uyumluluklar temel 5 grupta toplanabilir.

- Siber Güvenlik ile İlgili Teknik Bileşenler
- Veri ve Bilgi Güvenliği ile ilgili Ulusal Standartlara Uyum
- Sibet Güvenlik, E-Devlet gibi başlıklarda yayınlanmış ulusal rehberlere uyum
- Kamu Güvenli Ağı gibi milli altyapılara ve bunların gerektirdiği güvenlik kriterlerine uyum
- Veri güvenliği, kişisel veriler, katalog suçlarla mücadele gibi başlıklar başta olmak üzere veri tabanı bakımından uyum yükümlülüğü olan mevzuata uyum: İlgili temel mevzuat 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5070 sayılı Elektronik İmza Kanunu (e-Arşiv bakımından), 5651 sayılı kanun vd. ile bunlara bğlı yayımlanan tüm yönetmelikler ve ikincil mevzuat



4. Son aşamada, milli veri tabanına geçiş senaryosunun genel çerçevesinin belirlenmesi gerekmektedir:

a) Milli veri tabanının kullanım alanı geniş bir kitleye sahip olduğundan, geleneksel eğitim yöntemleri ile (seminer, eğitim toplantıları vs.) bu kitleye ulaşmak veya geleneksel materyaller ile (basılı ortam gibi) bu kitleye dinamik ve güncel bilgi aktarmak mümkün olmayacaktır. Dolayısıyla daha modern kanalları kullanma mecburiyeti karşımıza çıkmaktadır. Elektronik ortamda uzaktan eğitim alanında mevcut e-Devlet projelerinden UYAP ciddi bir deneyim ve birikime sahiptir. Benzer bir altyapı ve teknolojik yaklaşım ile milli veri tabanı için de e-eğitim içeriğinin oluşturulması gerekmektedir.

b) Öncelikle pilot aşama için seçilen kurumlar olmak üzere merkezi kamu kurumlarının bilgi işlem daire başkanlıklarındaki ilgili ekiplere milli veri tabanına geçiş ile ilgili teknik eğitimler sağlanmalıdır. Bu eğitimlerde ayrıca, mevcut yazılımlarda veri tabanına bağımlılığa sebep olan kodların nasıl uyumlu hale getirileceğine ilişkin bilgiler de sunulmalıdır.

c) Sistem kullanıma alındığında, karşılaşılan problemler ile ilgili destek almak üzere başvurulacak olan Teknik Çağrı Merkezi oluşturulmalıdır.

d) Uygulamaya kademeli olarak geçilmeli, pilot kurum seçilirken mevcutta farklı veri tabanı çözümlerini kullanan en az 3 kurum tespit edilmeli, veri taşınmasından

itibaren pilot süreç boyunca bizzat kurum bünyesinde, geçişten ve aktarımdan kaynaklı ilk ve temel problemlerin yerinde gözlenmesi ve çözüm üretilmesi amacıyla teknik ekipler konumlandırılarak destek sağlanmalıdır. Uyumlaştırma ve saha gözlem süreci, geçiş karmaşıklığına göre (kurum yazılımlarında veri tabanı bağımlı kodların ilgili yazılım ekipleri tarafından uyarlanmasına müteakip) en az 3 ay sürmelidir.

e) Son aşama olarak yaygınlaştırma fazında, önce merkezi kamu kurumları bilgi sistemlerinden başlayarak ve taşrada yer alan bölgesel bilgi sistemlerine kadar uzanarak tam yaygınlaştırma süreci tamamlanmalıdır.

Hazırlanma Tarihi: 01 Mart 2018

İletişim Bilgileri
E-Posta: afyonluoglu@gmail.com
Web Sayfası: http://afyonluoglu.org