~ 2. Gün – Etkinlik 1 Sunumu ~

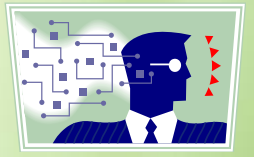
Bölüm 3: «Sistem Kavramı»

Bir Siber Güvenlik Macerası (BSGM) bir TÜBİTAK 4004 Doğa Eğitimi ve Bilim Okulları projesidir.

SUNUM İÇERİĞİ

Amaç: Sistem kavramının ne anlama geldiğini ve siber güvenlik kapsamında bir sistemi çözümlemenin neden önemli olduğunu anlamak.

- **Sistemin Tanımı**
- **Veri – Yazılım – Donanım Arasındaki Üçlü Sistem**
- **Siber Güvenlik Açısından Sistem Değerlendirmesi**

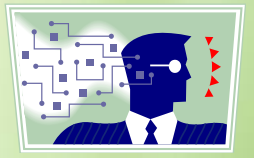


3.1. Sistemin Tanımı

▪ Genel olarak sistem, kendi içerisinde birbirleriyle ilişkili bileşenler barındıran ve çeşitli amaçlar doğrultusunda işleyen düzen bütününe denilmektedir. Sistemler kendi içerisinde alt-sistemler barındırabileceği gibi, başka sistemlerin alt-sistemleri de olabilmektedir.

▪ Sistemin ne olduğunu anlamak adına, aşağıda sıraladığımız birkaç sistem örneğine dikkatimizi verelim:

- Bir TV ya da buzdolabı kendi içerisine elektronik ve mekanik bir sistemdir.
- Evlerimizdeki su tesisatı bir tür sistemdir.
- Mobil telefonumuz bir tür sistemdir.
- Mobil telefonumuzda oynadığımız bir oyun aslında kendi içerisinde bir sistemdir.
- Trafik lambaları hep beraber bir sistemi oluşturmaktadır.
- Farklı derslere çalışırken benzer bir yöntem uyguluyorsak, bu yöntem aslında bir sistemdir.
- Okul, öğrencileri, öğretmenleri ve sınıflarıyla bir tür sistemdir.

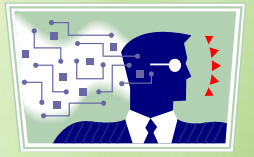


3.1. Sistemin Tanımı

- **Sıraladığımız örnekler neden birer sistemdir? Onları sistem yapan bileşenler neler olabilir?**

- **Gerçek hayattan başka sistem örnekleri verebilir misiniz? Verdiğiniz sistem örneklerinin temel bileşenleri nelerdir?**

- Anlaşılacağı üzere, sistem kavramı sadece somut unsurlar için değil, soyut nitelikteki her türlü düzen için kullanılabilmektedir. Problemlere çözümler üretmek ya da başka bir deyişle, istenilen birtakım görevleri yerine getirebilmek adına, sistem tasarlamamız gerekmektedir. Bu noktada, sistemler içerisinde etkin çözümler üretmek için de, bundan sonraki bölüm altında ele alacağımız algoritmalardan faydalanırız.

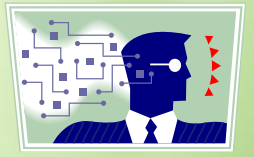


3.1. Sistemin Tanımı

▪ Gerçek hayatta kimi zaman belirli sistemlerin içerisine kendiliğimizden dâhil olur, kimi zaman ise sistemi kendimiz kurarız. Sistemlere bağlı başka sistemler tasarlarken ya da benzeri sistemler kurarken de var olan sistemleri iyi analiz etmemiz gerekir.

▪ Verdiğimiz sistem örneklerinden yola çıkarsak, özellikle somut sistemlerin analiz edilmesi ya da tasarlanması genellikle teknik bilgi ve beceriye ihtiyaç duyabilir. Ancak soyut sistemlerin analiz edilmesi ve tasarlanması için teorik anlamda belirli bir düzeye sahip olmamız yeterli olabilmektedir.

▪Konuyu siber güvenliğe bağladığımız zaman, günümüz koşulları altında karşımıza oldukça karmaşık ve sürekli değişebilen bir resim çıkmaktadır. Ama nereye, nasıl bakacağımızı bilirsek, siber dünyayla örülü bir çağda, güvenlik faktörünü doğru yerlere pekâlâ koyabiliriz.

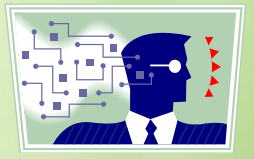


3.2. Veri – Yazılım – Donanım Arasındaki Üçlü Sistem

▪ Bilgisayar tabanlı sistemleri ve daha genel anlamda, yeter düzeyde gelişmiş sayısal sistemlerin işleyişini anlamlandırmak için kullanabileceğimiz en temel sistem, veri, yazılım ve donanım arasındaki üçlü sistemdir. 'Bermuda Şeytan Üçgeni' olarak da ifade edebileceğimiz bu sistem, öyle güzel bir düzene sahiptir ki, karşımıza çözülmesi gereken bir bulmacayı çıkarmaktadır. Bunu kısaca şöyle açıklayabiliriz:

- Donanımların çalışması için yazılımlara ihtiyacı vardır.
- Yazılımlar, görevlerini yapabilmek adına verileri (bilgiyi) kullanırlar.
- Yazılımlar, kendi başlarına bile birer veridir.
- Donanımları çalıştırabilmek adına uygun yazılımlar geliştirmemiz gerekir.
- Yazılımların doğru çalışabilmesi için uygun yapıda veriler sunmamız gerekir.
- Her üç bileşen de birbirine muhtaçtır.
- Üç bileşenden birinin var olmadığı bir sistem, günümüz siber dünyasıyla ilişkili değildir.

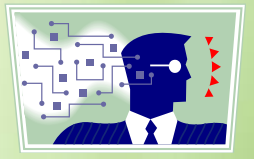
•Açıkladığımız bu üçlü sistem, özellikle siber güvenliği sağlama söz konusu olduğunda, bileşenlerin etkili bir şekilde eşgüdümünü gerekli kılmaktadır. Siber korsanlar cephesinde ise, bileşenler arası ilişkinin çok iyi bilinmesini ve art niyetli eylemler için de etkili çözümler üretilmesine ihtiyaç duymaktadır.



3.3. Siber Güvenlik Açısından Sistem Değerlendirmesi

▪ Siber güvenlik açısından sistem değerlendirmesi, odaktaki sistem ne olursa olsun, her türlü somut ve soyut bileşenin dikkate alınmasını gerektirmektedir. En güncel siber güvenlik yazılımlarına ve donanımlarına sahip olmanız, siber korsanlardan zarar görmeyeceğiniz anlamına gelmemektedir. Çünkü dünyanın en güncel ve sağlam yazılımları da donanımları da biz insanların emrine amade durumdadır ve kimi zaman dikkatimizden kaçan insanlar, bu yazılım ve donanımlarla en çok etkileşim kuracak unsurlar olabilmektedir.

▪ Şirket örneği ile devam etmemiz gerekirse, bilgi ve iletişim teknoloji kapsamında faaliyet gösteren bir şirket dünyaya tamamen kapalı olmadığı sürece (ki böyle bir durum pek mümkün değildir) illa ki çeşitli yan şirketlerle ve kişilerle etkileşim içerisindedir. Diğer yandan bu şirkette çalışanların her biri, kendi içerisinde sırları, zayıf noktaları olan insanlardır. Anlaşılacağı üzere, şirketin yazılımları, donanımları, çalışanları, işbirliği içerisinde olunan başka şirketler; şirketi bir sistem olarak ele aldığımızda sistem içi bileşenler olarak kabul edilmektedir. Şirketin kurulu olduğu binayı bile kendi içerisinde farklı dinamikler barındıran bir sistem bileşeni olarak kabul edebiliriz.



3.3. Siber Güvenlik Açısından Sistem Değerlendirmesi

- **Bir okul sisteminin temel bileşenleri neler olabilir? Birlikte tartışalım.**

- Açıklamalardan yola çıkacak olursak, siber güvenliği sağlanacak bir kurumun değerlendirilmesi gereken temel sistem bileşenlerini şöyle sıralayabiliriz:
- **İnsan:** İnsan faktörü siber güvenlik açısından o kadar önemlidir ki, sistem bileşeni olarak en tepede değerlendirmemiz yerinde olacaktır. Bir kurumda çalışan herkes ve hatta kurumun etkileşim içerisinde olduğu herkes, siber güvenliğin kaderini belirler niteliktedir.
- **Bilgi – Veri:** Kurum ile bağlantılı, korunan ya da korunmayan (gün yüzünde olan) her türlü bilgi ve veriler, sistemin temel bileşenleri arasındadır. En basitinden kurumdaki çalışanların sicil numaraları, dahili telefon numaraları, kurumun yemek saatleri ve kurum içi kullanılan bazı iletişim kodları bile siber korsanlar için altın değerinde olabilmektedir.

3.3. Siber Güvenlik Açısından Sistem Değerlendirmesi

- **Çevresel Faktörler:** Çevresel faktörlerden kasıt, kurumun etkileşim ve iletişim halinde olduğu başka kurumlar, insanlar ve somut unsurlardır. Kuruma temizlik hizmeti veren bir şirket, siber korsanların kolayca manipüle edebileceği bir unsur haline gelebilecektir. Benzer şekilde kurumun bulunduğu mahalle, yakınındaki binalar ya da çevresel düzenlemeler, fiziksel erişim adına siber korsanlar tarafından kullanılabilecektir.
- **Soyut Dinamikler:** Kurum içi işleyiş, çalışanlar arası hiyerarşik düzen, kurumun temeline zemin oluşturan ve somut olmayan her türlü soyut dinamik, temel sistem bileşenleri arasındadır.
- **Yazılım ve Donanım:** Siber korsan, hack ya da siber güvenlik kavramlarını düşündüğümüzde hemen aklımıza gelen bilgisayarlar, sayısal sistemler; yani yazılım ve donanımlar, tabi ki sistemin temel bileşenleri arasındadır.

3.4. Sistem Analizi ve Güvenli Bir Sistem Oluşturma

- Bir önceki başlık altında ifade ettiğimiz sistem yapısı ve bağlı bileşenleri dikkate aldığımızda, siber güvenliğin sağlanması noktasında ilgili bileşenler üzerinden bir analiz gerçekleştirmemiz gerektiğini sanırım anlamış durumdayız. Teknik olarak düşündüğümüzde, sistem analizi farklı çapta yaklaşımları barındırabiliyor olsa da, burada ifade edeceğimiz sistem analizi, mevcut sistem bileşenlerinin durumunu değerlendirmeye dayanmaktadır.

- Bu durumda, bir sistem olarak şirketimizin, bağlı olduğumuz kurumun ya da tamamen kendimizin siber güvenliğini sağlamak adına nasıl bir sistem analizi yapmamız gerekir; bunu tartışmamız gerekmektedir.

3.4. Sistem Analizi ve Güvenli Bir Sistem Oluşturma

- Detaylardan arınmak suretiyle, sistemin iyi bir analizini yapmak için şu adımların takip edilmesinin faydalı olacağını düşünebiliriz:
  - Çalışanların siber güvenlik açısından eğitim düzeyinin değerlendirilmesi,
  - Sistem ile ilişkili çevresel faktörlerin risk durumunun anlaşılması,
  - Yazılım ve donanım tabanlı bileşenlerin mevcut durumunun, siber güvenliği sağlamaları açısından başarım durumlarının ve birbirleriyle olan ilişkilerin değerlendirilmesi,
  - Sistemde mevcut olan siber savunma odaklı önlemlerin değerlendirilmesi,
  - Sistem için hayati önem taşıyan, başta veri olmak üzere, somut varlıkların güvenlik düzeyinin değerlendirilmesi,
  - Alternatif olumsuz senaryolar karşısında, sistemin mevcut durumunun ne kadar sağlam olduğunun değerlendirilmesi.

3.4. Sistem Analizi ve Güvenli Bir Sistem Oluşturma

- İfade edilen eylemlerden yola çıkmak suretiyle yapılan genel bir sistem analizi, sistemin güvenli hale getirilmesi için neler yapılması gerektiğine de ışık tutacaktır. Ama biz yine de, sistem güvenliğini sağlama noktasında yapılabilecekleri kısaca sıralayalım:
- Çalışanların siber güvenlik açısından belli aralıklarla test edilmesi ve güncel eğitimlerle desteklenmesi,
- Çevresel faktörlerin dikkatle seçilmesi, mevcut faktörlerin sık sık değerlendirilmesi,
- Dış faktörlere fazla bağlı kalmaktansa, mümkün olduğunca sistem için bileşenlerle çözümler üretilmesini sağlamak,
- Siber güvenliği sağlayacak yazılımsal ve donanımsal bütün önlemlerin alınmasını sağlamak,
- Siber güvenliği sağlayacak etkin personel ve takıma sahip olmak,
- Sistem içerisinde mevcut yazılım ve donanımların zafiyetlere karşı sürekli denetim altında tutulması,
- Sisteme yabancı unsurların sistem ile etkileşimine mümkün olduğunca izin vermemek,
- Sistem için faaliyetlerde mümkün olduğunca çapraz onaylı süreçlere yer vermek,
- Sistem dışına bilgi / veri ve benzeri unsurların çıkmasına engel olacak önlemler almak,
- Sistemin genel dinamiklerinin ‘gerçekten’ farkında olmak,
- Teknolojiye kapalı olmamak,
- Teknoloji kültürüne ve gelişmelere karşı daima açık ve duyarlı olmak.

3.4. Sistem Analizi ve Güvenli Bir Sistem Oluşturma

- **Bir şirketiniz var. Şirketiniz dışarıdan temizlik ve gıda hizmeti alıyor. Şirket ortamı çok fazla farklı insanın etkileşimine de açık durumda. Sistem güvenliğini sağlama noktasında ne gibi önlemler alırsınız?**

~ 2. Gün – Etkinlik 1 Sunumu ~

Bölüm 3: «Sistem Kavramı»

Sunum Sonu ☺
Sorularınızı sormaktan çekinmeyiniz ☺

Bir Siber Güvenlik Macerası (BSGM) bir TÜBİTAK 4004 Doğa Eğitimi ve Bilim Okulları projesidir.