YMT 311-Bilgi Sistemleri ve Güvenliği

Siber Bilgi Güvenliği

Konu Başlıkları

- Genel Bakış ve Terminoloji
- Gündemdekiler
- Mevcut Durum Analizi
- Güncel Tehdit ve Tehlikeler
- Nasıl bir SBG? Öneriler
- Sonuç ve Değerlendirmeler

Tanım : Siber Güvenlik?

- “Kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü” olarak tanımlanıyor.

Bilgi Nedir ?

- İşlenmiş veridir.
- Bir konu hakkında belirsizliği azaltan kaynaktır (Shannon).
- Kişi/kurum/kuruluşlar için önemli ve değerli olan bir kaynaktır ve korunması gerekir.
- Veri (data), bilgi (information), ve özbilgi (knowledge)

Bilgi Nedir ?

- Boşlukta ve zamanda yer kaplar.
- Gürültü çıkarmadan hareket edemez.
- Bilginin hareket etmesi için enerji gerekir.
- Bilgi yaşam ve herhangi bir düzenli etkinlik için gereklidir.
- Bilgi hem maddesiz biçim; hem biçimsiz maddedir.
- Işık gibi, bilgi'nin de ağırlığı vardır. Bir GB, bir parmak izinden daha az ağırlıktadır.
- Bilgi zaman içinde hareketli veya donmuş olabilir.
- Bilgi, bir soruya tatmin edici, belki de rahatsızlık verici cevaptır.
- Bir taşın ağırlığı ile bunu tanımlamak için gerekli bilgi birbirine eşittir.
- Bilgi, katı hale sahiptir; donarak katılaşır (depolama).
- Bilgi, sıvı hale sahiptir; akar (iletişim).
- Bir yerlerde bilgi hareket eder; evren gümbürder ve gerçeği gürler.
- Maddeden farklı olarak bilgi aynı anda birden fazla yerde olabilir.
- El sıkışma bir bilgidir. Bir baş sallama, bir bakış, bir iç çekiş.
- Bilgi, rastsallık denizinde parlar.

BİLGİ (Veri)?

- İngilizce karşılığı olarak “data”,
- Latince “datum” (çoğul şekli “data” ve “vermeye cesaret etmek” fiilinin geçmiş zamanı, dolayısıyla “verilen şey”)
- Latince “data” (dedomena) kavramının M.Ö. 300 yıllarında Öklid’in bir çalışmasında geçtiği bildirilmektedir.
- Dilimizde de verilen şey anlamında, “veri” olarak kullanılmaktadır.
- Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.

BİLGİ (Bilgi)?

- Bilgi, verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir.
- Veri ve ilişkili olduğu konu, bağlamı içinde bilgi üretecek şekilde bir araya getirilir.
- İşlenmiş veri olarak da ifade edilebilecek bilgi, bir konu hakkında var olan belirsizliği azaltan bir kaynaktır.
- Veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmelerin) çıktısıdır.

BİLGİ (Özbilgi)?

- Tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır.
- Verileri bir araya getirip, işlemek bilgiyi oluştursa da; özbilgi, kullanılan bilgilerin toplamından daha yüksek bir değer sahip bir kavramdır.
- Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir.

Veri-Bilgi-Özbilgi ?

- Veri (data), bilgi (information), özbilgi (knowledge) basamaklarıdır.
- Gerçeklik (reality) ile hikmet (wisdom) arasında gösterilen bu merdivenin basamakları
- Çoğu durumda her basamak, atlanmadan teker teker geçilir.
- Yukarıya çıktıkça elimizdeki şeyin miktarı azalırken; değeri artar.
- Yine yukarıya çıktıkça bir sonraki basamağa adım atmak daha da zorlaşır ya da daha çok çaba ister.
- Genel olarak bilimin getirdiği yöntemlerden ölçme ile,
- eldeki gerçeklikten **veriye ulaşılır;**
- ispat ile, veriden **bilgiye ulaşılır ve**
- kavrayış ile, bilgiden **özbilgiye ulaşılır.**
- Bir özbilginin gerçeklik haline dönüştürülmesi de mümkündür. Bunun için yönetim biliminden yararlanılır.

Güvenlik?

- Karşılaşılabilecek tehditlere karşı önlem alma
- Kişi ve kurumların BT kullanırken karşılaşabilecekleri tehdit ve tehlikelerin daha önceden analizlerinin yapılarak gerekli önlemlerin alınmasını sağlama

Bilgi Güvenliği?

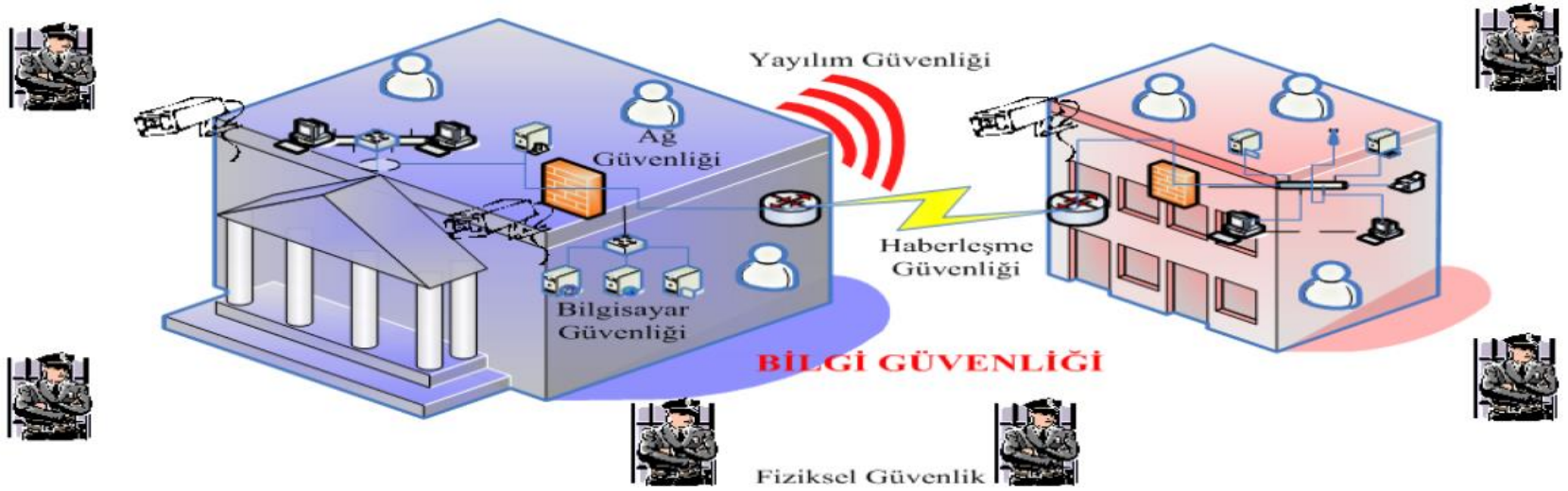
- Bilginin değerli veya değersiz olduğunu belirlemek veya bilginin taşıdığı değeri ölçmek, en az bilginin kendisi kadar önemlidir.
- Bilgiyi değerlendirirken bilginin kalitesini gösteren özelliklere bakılması gerekir.
- Doğruluk, güncellik, konuyla ilgili olma, bütünlük ve öz, gereksinimlere uyum gösterme, iyi sunulma ve fiziksel ve idrak yolu ile erişim gibi ölçütler bilginin kalitesini belirleyen etmenlerden bazılarıdır.
- Bilginin çok önemli bir varlık olması, ona sahip olma ile ilgili bazı konuların düzenlenmesi ve yeni şartların getirdiği özelliklere göre ayarlanmasını gerekmektedir.
- Bilgi en basit benzetme ile para gibi bir metadır.

Bilgi Güvenliği?

- Dünya gündeminde bir konudur.
- Bilginin bir varlık olarak hasarlardan korunması
- Doğru teknolojinin doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda istenmeyen kişiler veya sistemler tarafından elde edilmesini önleme

Bilgi Güvenliği?

- Bilgiye sürekli olarak **erişilebilirliğin sağlandığı bir ortamda,** bilginin göndericisinden alıcısına kadar **gizlilik** içerisinde,bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden **bütünlüğünün sağlanması ve güvenli** bir şekilde iletilmesi **sürecidir.**



Siber Bilgi Güvenliği ?

- Bilgi Güvenliği nerede sağlanmalı ?
  - Üretim
  - Erişim
  - İşleme
  - Depolama
  - Aktarma
  - Yok etme

Siber Güvenliğin Temel Hedefi?

- Kurum ve kuruluşların veya en genel anlamda ulusların bilgi varlıkları ve kaynaklarını hedeflenen amaçlar doğrultusunda organizasyon, insan, finans, teknik ve bilgi değerlerini dikkate alarak, varlıkların ve kaynakların başlarına **KÖTÜ BİR ŞEYLER GELMEDEN korumaktır.**

Tanım (ABD Başkanı Barack Obama)

- “Ülke olarak karşılaşılan çok ciddi ekonomik ve ulusal güvenlik sağlama hedeflerinden birisi olup hükümet veya ülke olarak henüz tam anlamıyla önlem alamadığımız bir hususdur.” “Amerika’nın sayısal altyapısını kapsamlı olarak güven altına alma yaklaşımlarının geliştirilmesi ve bilgi ile haberleşme altyapısının savunulmasına yönelik olarak federal çözümlerin gözden geçirilmesi” emrini verir. **"21. yüzyılda Amerika’nın ekonomik zenginliği, siber güvenliğe bağlı olacaktır."** ***Mayıs 2009***

Ülkemizdeki Tanımlar..

Ulaştırma Bakanı Sn. Binali Yıldırım

- “bilgi sistemi güvenliğinde ortak akıl ve ortak hareketle hattı müdafaa yerine sathı müdafaanın başarılı bir şekilde gerçekleştirilme girişimi”,
- “devletin birinci dereceden ilgilenmesi gereken bir mesele olarak görüyoruz.”
- “siber savaş tehdidine karşı hazırlıklı olmanın, kurumların bilgi sistemi güvenliği olaylarına müdahale yeteneği ile kurumlar arası koordinasyon yeteneğini tespit ederek, alınacak önlemler ve bilincinin arttırılmasını amaçlamak”

Faydalar

1.Zamandan bağımsızlık
2.Mekandan bağımsızlık
3.Hız
4.Verimlilik
5.Gelişim/Değişim
6.Hayatı kolaylaştırıyor
7.Yönetmeyi kolaylaştırıyor
8.Denetlemeyi kolaylaştırıyor

Zararlar

1. Bilmeyenler için kontrolü zor..
2. Açıklarını bilenleri öne çıkarıyor..
3. Kötülere çok yardımcı oluyor..
4. Bilmeyenlere hayatı dar ediyor..
5. Bağımlılık yapıyor..
6. Kişisel gelişimi kısmen olumsuz etkiliyor..
7. Gelişmemiş toplumları köleleştiriyor..

60 saniyede neler oluyor? -1

- 168 milyon e-posta gönderiliyor.
- 1500’den fazla blog iletisi yayımlanıyor.
- 70’den fazla domain adı alınıyor.
- Flicker üzerinden en az 6600 fotograf paylaşılıyor.
- Skype üzerinden 370000 dakika konuşuluyor
- Scribd üzerinden en az 1600 okuma gerçekleşiyor.
- Pandora’da 13000 saatten fazla müzik akıyor.
- 13 000 IPhone uygulaması indiriliyor..

60 saniyede neler oluyor? -2

Facebook

- En az 695000 Facebook durum güncellemesi yapılıyor.
- 79364 duvar iletisi yazılıyor.
- 510040 yorum yapılıyor.

Twitter

- 320 Twitter hesabı açılıyor
- En az 98000 Tweet atılıyor.
- 13000 fazla iPhone uygulaması indiriliyor.

60 saniyede neler oluyor? -3

Youtube

- 600000’den fazla yeni görüntü yayımlanıyor.
- Dünya genelinde YouTube'de kalma süresi 25 saatten fazla.

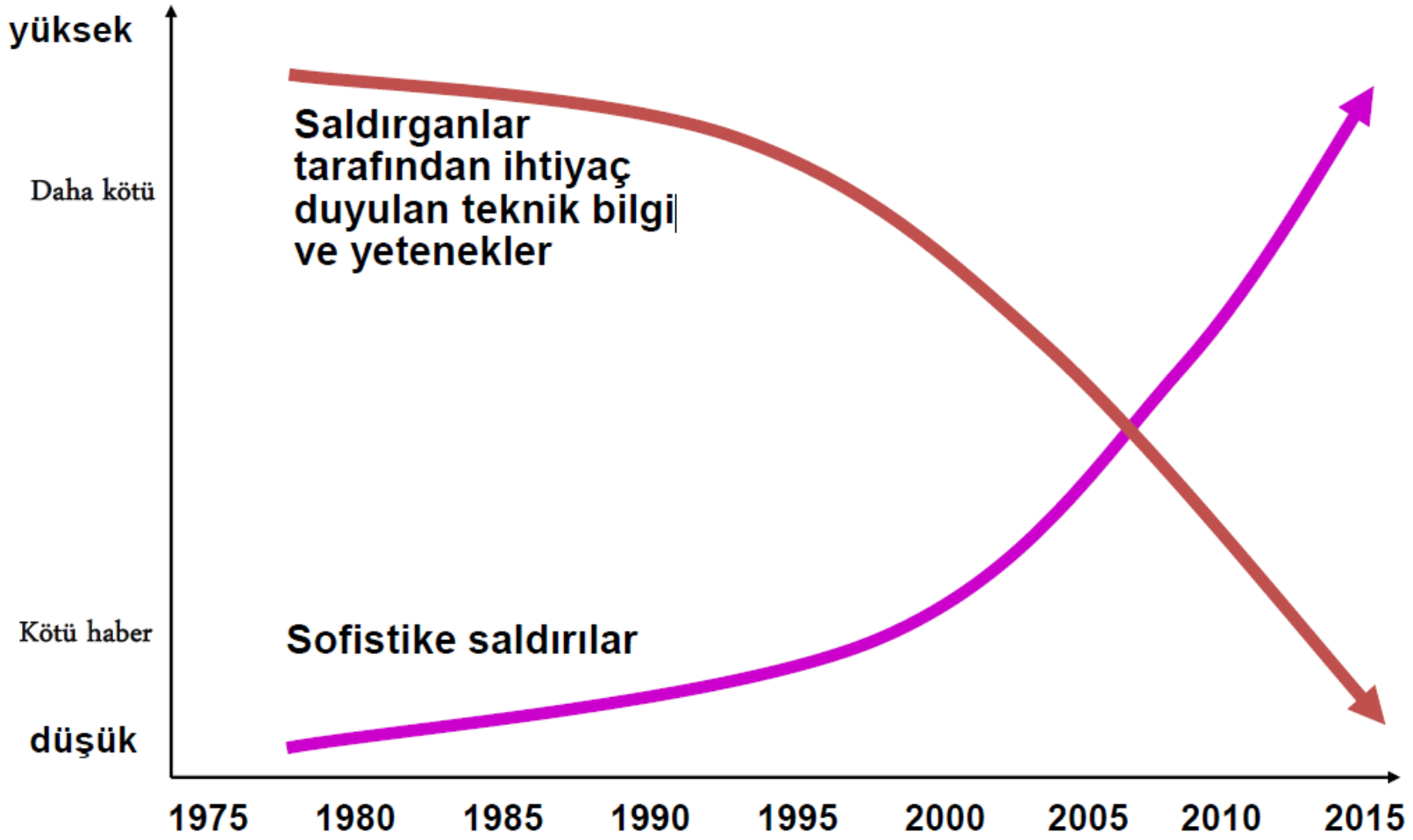
Yahoo

- en az 100 soru ve 40 cevap Yahoo’da akıyor.

LinkedIn

- LinkedIn’e 100’den fazla profil ekleniyor.

Siber Ortamlar



Siber Ortamlar

Ulusal Askeri Stratejiler doğrultusunda;

- 15 Kasım 1940'da 500 savaş uçağı İngiliz Coventry şehrini bombaladı.
- Kod adı "Ay Işığı Sonatı" (Ludwig van Beethoven)
- Bu saldırı Enigma kullanılarak şifrelenmişti.
- Yüzlerce ölü ile beraber şehrin üçte ikisi yıkıldı.
- Kendi bilgi ve bilgi sistemlerimizi etkin bir şekilde kullanırken amaç savaşı kazanmak

Siber Ortamlar

- 1952’de Amerikan Ulusal Güvenlik Ajansı (NSA)
- Amerikan karar vericilere ve askeri liderlere zamanında bilgi sağlamak için Başkan Truman tarafından kurulmuş 1960'da Rusya'ya iltica eden iki NSA görevlisi ABD'nin 40 ülkenin haberleşmesini dinlediğini açıklamışlardır.

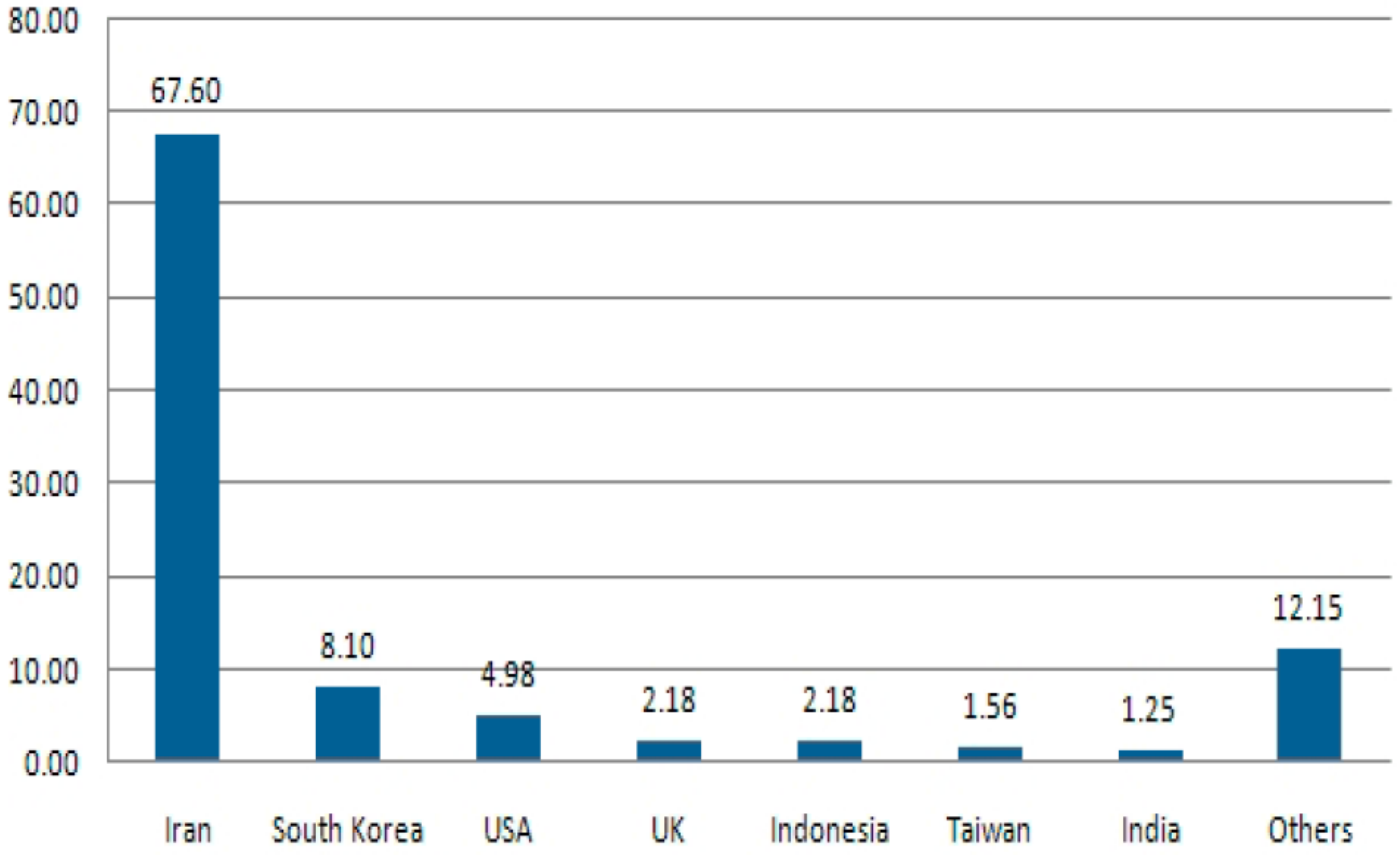
Siber Ortamlar

- Bilgiye her yerden erişilebiliyor..
- Arama motorları var..
- Sosyal ağlar..
- Sanal ortamda bir savaş var..
- İnsan beyni okunabiliyor..
- Akla hayale gelmedik yaklaşımlar geliştiriliyor..
- İzleme hat safhada..

STUXNET Neler Öğretti

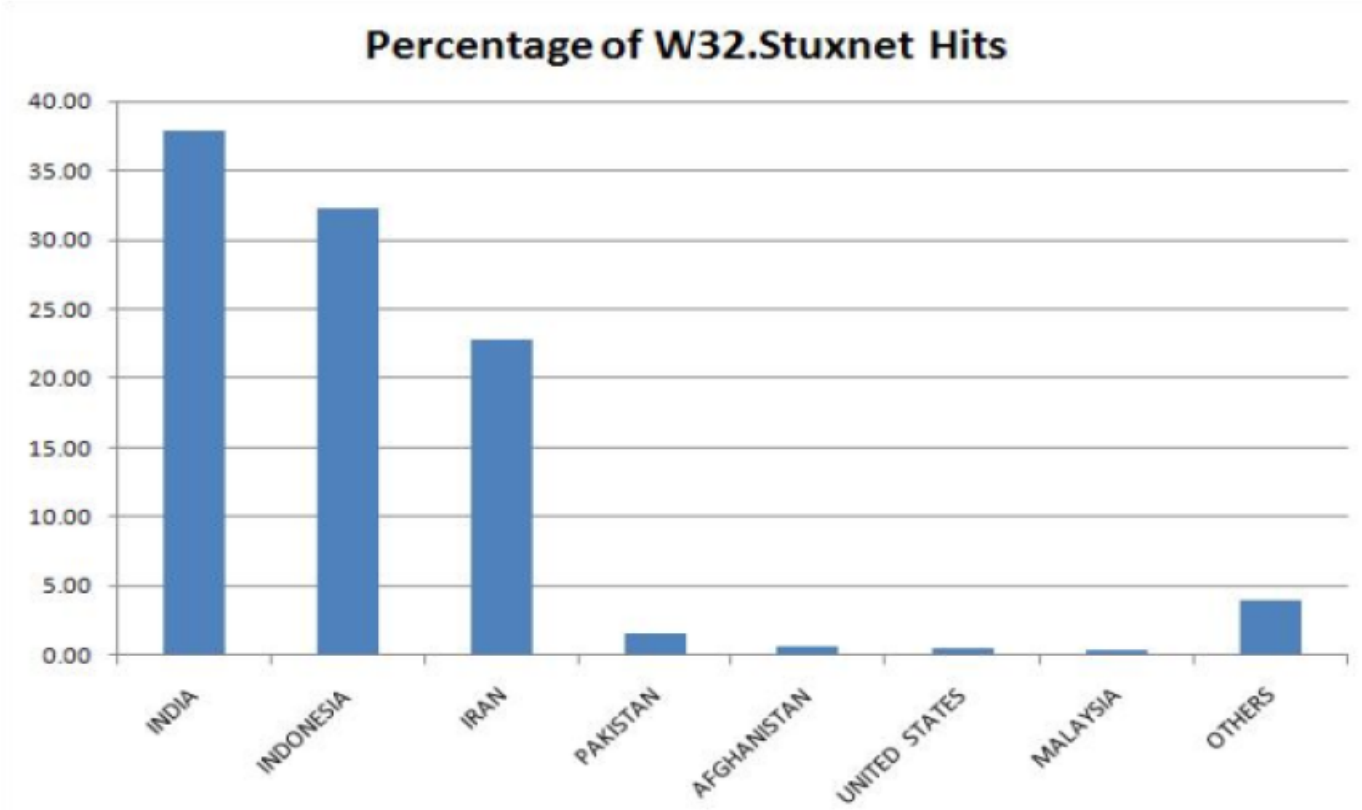
- Ezber bozan bir yaklaşım
- Altyapıya saldırı için planlanmış
- Önemli sistemlerin korunaklı olmadığı
- Kolaylıkla sistemlere zarar verilebileceği
- Bir ülkenin nükleer programını durdurabilecek kadar önemli
- Spekülasyon ile ülkelerin prestijlerine zarar verme

Etkilenen Sistemler



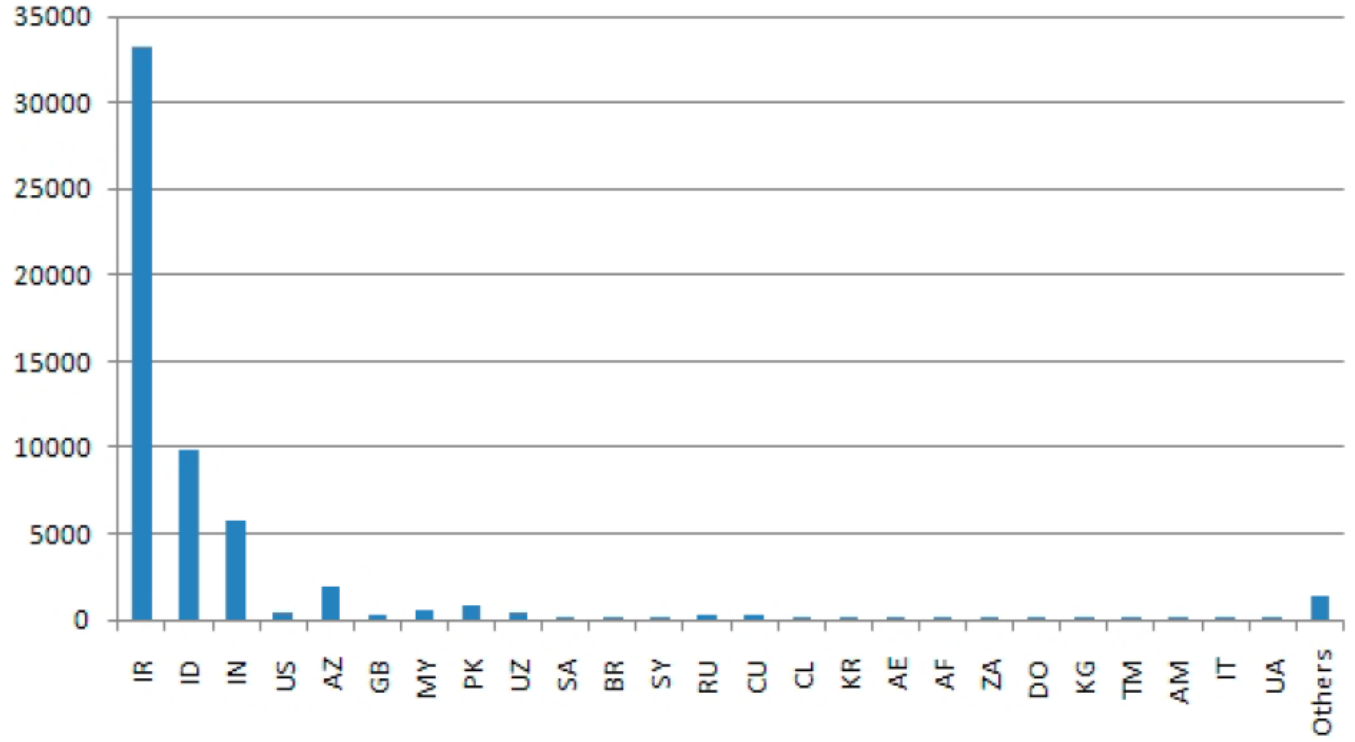
Etkilenen Sistemler

- USB Sürücülerde Yayılma

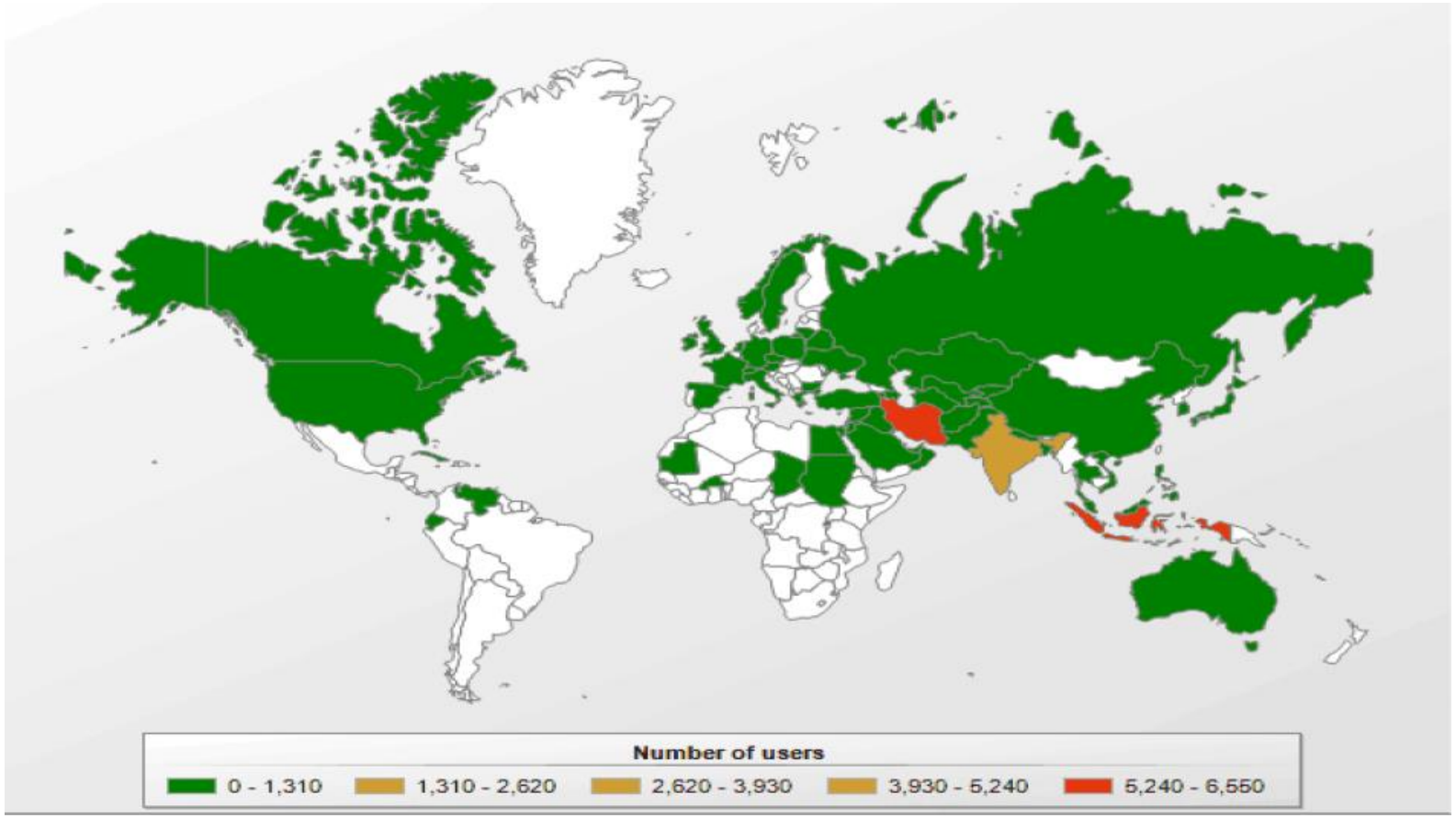


Etkilenen Organizasyonlar

- WAN IP



Stuxnet’den Dünya Çapında Etkilenme



Siber Tehditlerin Amaçları

- Sisteme yetkisiz erişim
- Sistemin bozulması
- Hizmetlerin engellenmesi
- Bilgilerin
  - Değiştirilmesi
  - Yok edilmesi
  - İfşa edilmesi
  - Çalınması

Siber Ortamlar

İyilerin ve Kötülerin amansız savaşı

- Saldıran Taraf
- Savunan Taraf

Siber Ortamlar

- **Saldıran Taraf**
  - Saldırılar artmakta
  - Saldırı bilgi seviyesi hızla azalmakta
  - Kötücül kodlar gelişerek ve değişerek hızla yayılmakta
  - Organize sanal suç örgütlerini kurma
  - İyilerden hep bir adım önde

Siber Ortamlar

Savunan Taraf

- Güvenliğin en zayıf halkası
- Bilgisizlik, ilgisizlik, hafife alma,
- %100 Güvenliğin sağlanamaması **%99,9 Korunma + %0,1 Korunmasızlık=%100 güvensizlik**
- Bilgi birikimi (Yatırım, Eğitim ve zaman)
- Kişilere güven duygusu
- E-dünyanın doğasında olan güvensizlik

Siber Ortamlar

Siber Bilgi Güvenliği ?

- Üretim
- Erişim
- İşleme
- Depolama
- Aktarma
- Yok etme

Siber Güvenlik Kültürünün Oluşturulması

Bireysel Stratejiler

- Tehlikelerin farkında olmak
- Çok katmanlı bir savunma mekanizması oluşturmak
  - Çoklu araçlar
  - Yama programları
  - Güncellemeler
- Sosyal medyada gizlilik seçeneklerini iyi değerlendirmek
- Verilerinizin nerede olduğundan emin olun
- Kötü çocuk gibi düşünün
- Çocukların erişilebilirliğini sınırlayın

CIA

- Confidentiality – Gizlilik
  - Bilgi ne anlama geliyor
- Integrity – Bütünlük
  - Değişim olmadığı doğrulanabiliyor mu?
- Availability – Geçerlilik
  - İhtiyaç duyulduğunda bilgiye erişilebiliyor mu ?

<u>Ek özellikler</u>

- Non-repudiation – İnkar edememe
- Authentication -Yetkilendirme

Sonuç

- Bilgi Güvenliği **ürün veya hizmet değildir.**
- İnsan faktörü, teknoloji ve eğitim unsurları üçgeninde **yönetilmesi zorunlu olan karmaşık süreçlerden oluşan, süreklilik arz eden bir süreçtir.**
- Üç unsur arasında tamamlayıcılık olmadığı sürece **yüksek seviyede bir güvenlikten bahsedebilmek mümkün değildir.**
- Yüksek seviyede E-Devlet güvenliğinden bahsedebilmek için **Kurumsal ve Bireysel anlamda Bilgi Güvenliğinin gerekleri yerine getirilmelidir.**