Bilgi Güvenliğinde İnsan Faktörü ve ISO 27001

Kerim Yüksel, M.Sc.
VBASE – Bilgi Güvenliği Çözüm Ortağı

KİDDER, 11/05/2018

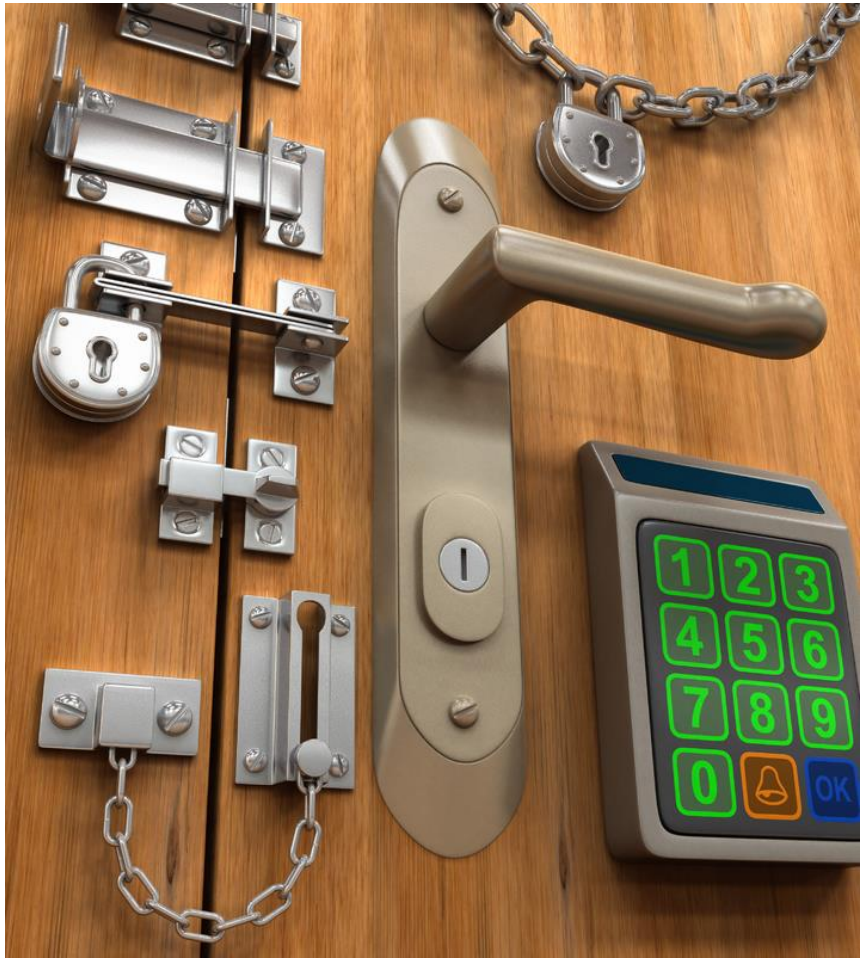
Sunucu?

- Kerim Yüksel M.Sc., Elektrik ve Endüstri Mühendisliği, İTÜ
  - **Master of Service Academy** kurucu ve yöneticisi
  - **VBASE** – Bilgi güvenliği çözüm ortağı
  - **İstanbul Bilgi Üniversitesi –** Öğretim görevlisi
  - **İngiliz Standartları Enstitüsü (BSI) –** Sözleşmeli eğitmen, danışman ve denetçi**,** ISO 27001, ISO 20000 ve ISO 22301 standartları
  - İş hayatına 1999 yılında **Alcatel'de saha mühendisi** olarak başladı
  - Çalıştığı firmalar;
    - **Alcatel Teletaş** – Saha Mühendisi & Takım Lideri, 1999 - 2004
    - **Borusan Bilişim** – Proje Yöneticisi, 2004
    - **Turkcell, Global Bilgi** – Servis Destek Yöneticisi, 2005 – 2007
    - **Noventum GmbH** – Kıdemli danışman, ITSM Bölüm Yöneticisi, 2007 – 2014
    - **OBSS** – Kıdemli İş Geliştirme Yöneticisi, ITSM Danışmanı, 2014 – 2016

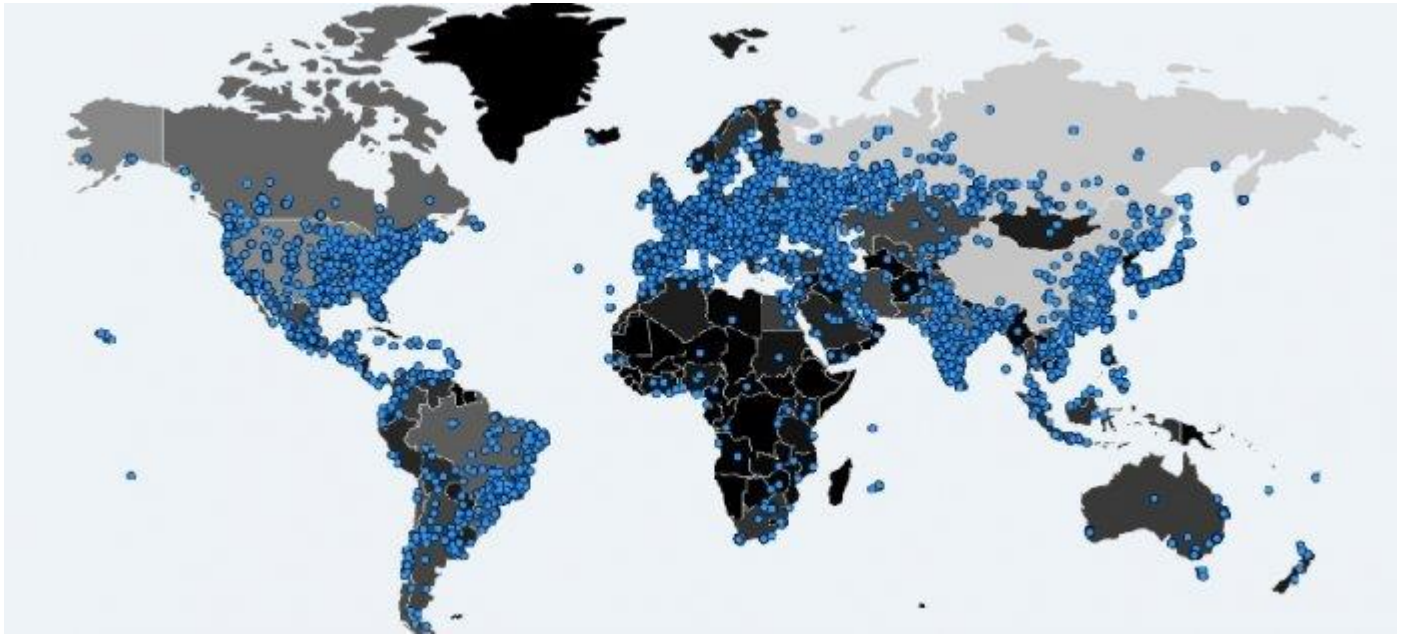
Çocukluğumuza inelim…

Uyarı: Kimlik doğrula(yama)ma yöntemiyle yüksek doz hacking içerir!

Kapımız kilitli, ama….



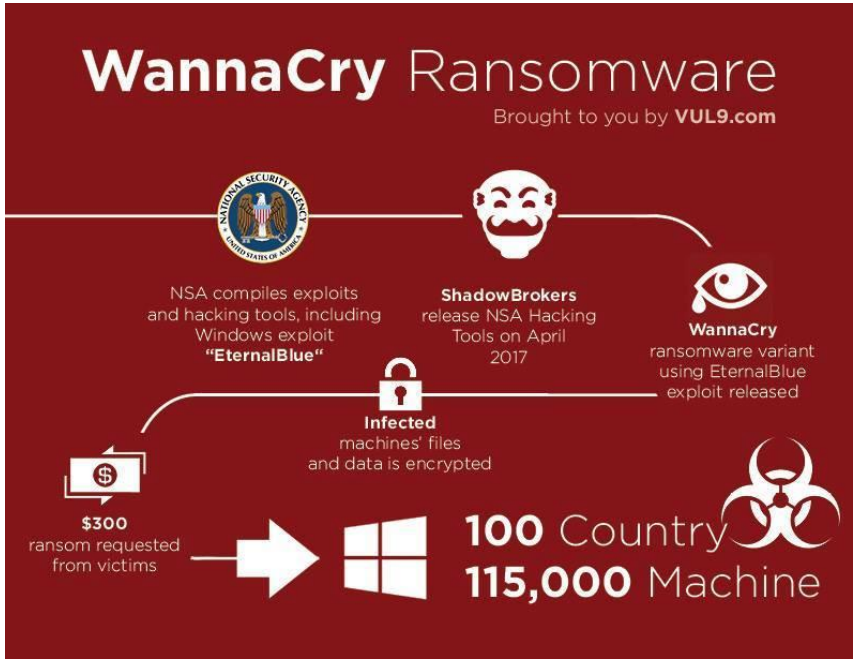
Açtığımız e-postalar….



Wanna Cry???

- İngiltere Sağlık Hizmetleri NHS, Nissan, Renault, Rusya ve Almanya Demiryolları
- FedEx, Hindistan polisi, Çin üniversite ve bankaları, Hitachi…….
- Toplam zarar yaklaşık 5 Milyar USD
- Siber suçların yıllık maliyeti 600 Milyar USD
- **2019'da siber suçların yıllık maliyeti???**

Kim tasarlıyor bunları??



EternalBlue???

- WannaCry ve Petya gibi zararlı yazılımların kaynak kodu.
- Asıl adı EternalBlue MS17-010
- Microsoft'un dosya ve yazıcı paylaşımı için geliştirdiği yöntemi kullanır
- **NSA'in (National Security Agency) uzak bilgisayarları ele geçirmek için tasarladığı bir çözüm…**

Nereye varır bu iş??

- Endüstriyel otomasyon tesislerini uzaktan manipüle edebilir.
- 2010'da İran'ın uranyum zenginleştirme programını durdurdu.
- Kendi karar mekanizmaları ile programlandığı şekilde hedefe ilerler.
- 100 milyon USD bütçe ile geliştirilen bir zararlı mühendislik harikası.
- **Kaynak kodu bugün Dark Web'de 50 – 100 bin USD'ye satılıyor.**

Peki ne yapmalı??

ISO/IEC 27001:2013…

- Risk yönetimi bazlı bir Bilgi Güvenliği Yönetim Sistemidir.
- Kurumun bilgi varlıklarını Gizlilik, Bütünlük, Erişilebilirlik açılarından korumayı hedefler.
- Madde 4 – 10 arası temel kaideler ve 114 adet kontrol içerir

Ne diyor ISO 27001??

Ana maddeler;

- Madde 4: Kuruluşun bağlamı
  - Neredeyiz? Kimlerle çalışıyoruz? İlgili tarafların ihtiyaç ve beklentileri nelerdir?
- Madde 5: Liderlik
  - Lider desteği olmadan olmaz. Kurumsal rol, sorumluluk ve yetkiler verilmiş ve destekleniyor olmalı
  - Herkesin durumun farkında olması sağlanmalı
- Madde 6: Planlama
  - Risk yönetimi. Risk değerlendirme, işleme, planlama

Ne diyor ISO 27001??

Ana maddeler;

- Madde 7: Destek
  - Yeterlilik, eğitim, farkındalık
  - İletişim, yazılı bilgiler.
- Madde 8: Operasyon
  - Günlük operasyon sırasında oluşan durum ve risklerin yönetimi
- Madde 9: Performans değerlendirme
  - Ölçme, iç tetkik ve yönetimin gözden geçirmesi
- Madde 10: Sürekli iyileştirme
  - Uygunsuzluk ve düzeltici faaliyet, sürekli iyileştirme

Ne diyor ISO 27001??

Bazı kontroller;

- A.6.2 Mobil cihazlar ve uzaktan çalışma
- A.7 İnsan kaynakları güvenliği
  - A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi
  - A.7.2.3 Disiplin prosesi
- A.8 Varlık yönetimi
  - A.8.1.2 Varlıkların sahipliği
  - A.8.1.3 Varlıkların kabul edilebilir kullanımı
- 8.3 Ortam işleme
  - 8.3.1 Taşınabilir ortam yönetimi
  - 8.3.2 Ortamın yok edilmesi

Ne diyor ISO 27001??

Bazı kontroller;

- A.9 Erişim kontrolü
- A.11 Fiziksel ve çevresel güvenlik
- A.12 İşletim güvenliği
  - A.12.2 Kötücül yazılımlardan koruma
- A.13.2 Bilgi transferi
- A.15 Tedarikçi ilişkileri
- A.16 Bilgi güvenliği ihlal olayı yönetimi
- A.18.2 Bilgi güvenliği gözden geçirmeleri

Teşekkürler & Sorular…