Cyber Recovery Solution (CRS)
Siber Kurtarma Çözümü

Şevket Kaan Ağaoğlu
DPS Yöneticisi – Türkiye

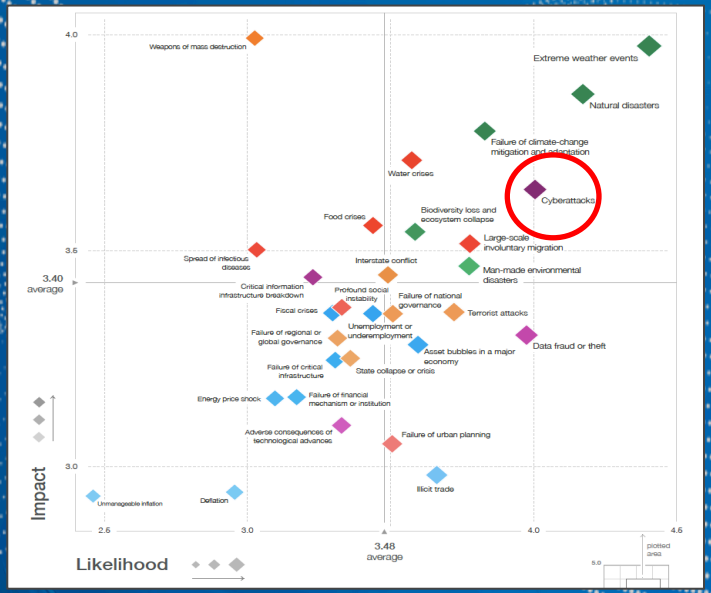
+90 541 4974330
Sevket.agaoglu@dell.com

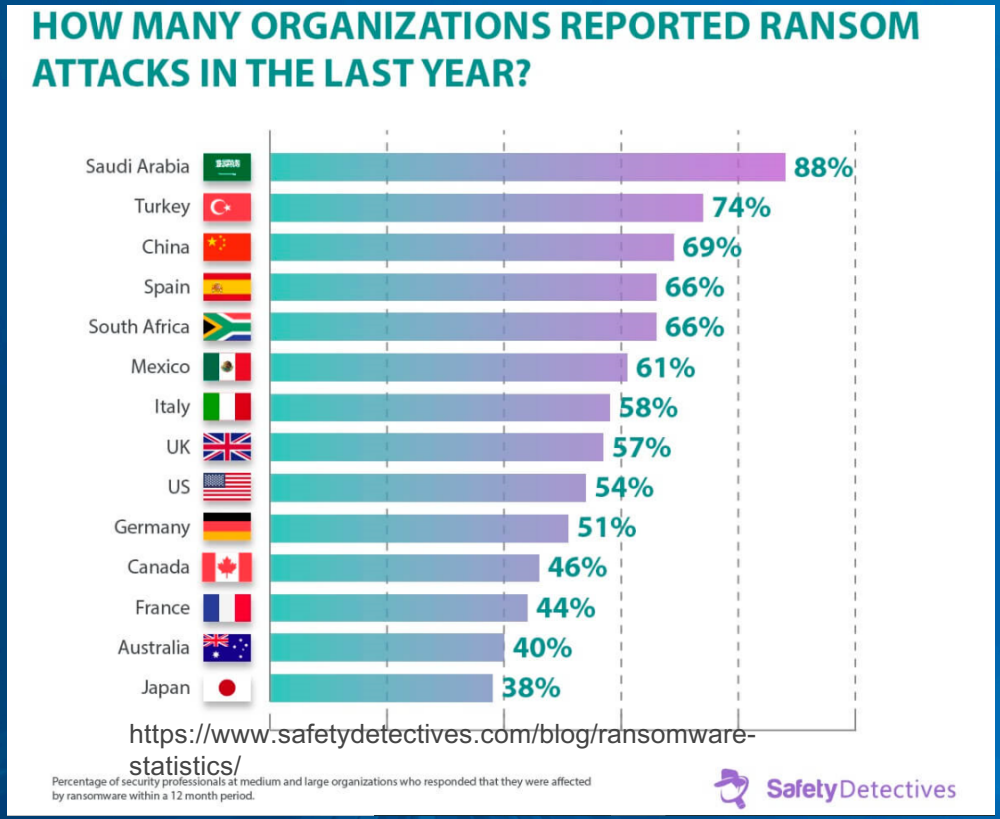
DELL Technologies

Siber Saldırılar Risk Sıralamasında 3. sırada

Dünya Ekonomik Forumu (World Economic Forum) 2018 Global Risk Analiz Anketi

Kurumların maruz kaldığı siber saldırılar son 5 senede iki katına çıktı. Geçmişte olmaz denilen tarzda saldırılar bugünün yeni normali haline dönüştü.





Siber Dayanıklılık: Hukuki ve Regulatif Direktifler

"Hava boşluğu arkasında korunan bir yedekleme altyapısı…"

"Gizlilik, her an çalışabilir olmak, bütünlük ve dayanıklılık "

"Yedeklerinizi çevrimdışı ve ulaşılamaz halde koruyun"

"Yedeklerinizin yedeğini aldığınız ağlara bağlı olmadığından emin olun"

Korunması Gereken Kritik Veri Örnekleri

Kimlik, Doğrulama ve Güvenlik

- Sertifikalar
- Active Directory / LDAP
- DNS sunucu verileri
- Loglar ve olay raporları

Şebeke Verileri

- Switch / router konfigurasyonları
- Firewall / load-balancer ayarları
- IP Servis dizaynı
- Access Control konfigurasyonları
- Firmware / Microcode / Patches

Veri Depolama / Yedekleme

- Yedekleme Kataloğu
- SAN / Array konfigurasyonları
- Sanal Storage ayarları
- Donanım konfigurasyonları

Kuruma ait Fikir Hakları olan veriler

- Kaynak kodları
- Özel algoritmalar
- Developer kütüphaneleri

Uygulama Geliştirme ve Barındırma Araçları

- Fiziksel / sanal platform verileri
- Dev Ops araçları & otomasyon scriptleri
- Firmware / Microcode / Patches
- 3. parti yazılım
  - Altın kopyalar
  - Konfigürasyon ve ayarlar

Dökümantasyon

- CMDB / varlık yönetim kopyaları
- FKM ve Siber Kurtarma Prosesleri
- İnsan Kaynakları verileri Ve Kontak bilgileri
- Olay müdahele prosesleri ve raporları

Siber Saldırganların Evrimi

Değişik Motivasyon, Teknik ve Hedefler

ADİ SUÇ	İÇ DÜŞMAN	ESPİYONAJ	HACKTİVİZM	TERÖRİZM	SAVAŞ
Hırsızlık ve Finansal Kazanç için Saldırı	Kurum içinde güvenilen kişilerin kişisel kazanc veya ideolojik sebeplerle kuruma yapılan saldırılarda rol oynaması. IT erişimleri olduğu için çok kritik.	Rakip kurumlar veya devletler çok değerli verileri çalabiliyor	Politik veya sosyal sebeplerden dolayı kurumlara yapılan saldırılar	Korku salmak için yapılan sabotaj ve saldırılar	Siber saldırı gücü olan devletlerin karşı devlet veya kurumlara saldırısı (NotPetya)

vodafone TR 3G 10:32 %90

bbc.com — Private

Australia

Australia cyber attacks: PM Morrison warns of 'sophisticated' state hack

2 hours ago

Scott Morrison said the "malicious" activity had been increasing over months

Australia's government and institutions

Veri Kurtarmaya/Siber Kurtarmaya dair bazı yanlış algılar

Veri Şifreleme (Encryption)

-Yıkıcı Ransomware saldırılarında koruma sağlamaz.
-Veri Koruma için kullanılır. Saldırıdan sonra geri dönmeye faydası olmaz

Daha Çok Güvenlik

-Her zaman daha çok güvenlik koruma seviyenizi arttırmaz
-İç saldırılar, insan hatası ve sistem karışıklığı güvenlik seviyesinin arttırılması ile çözülemeyebilir.

Teyp Kopyaları

-Geri dönüş haftalar boyu sürebilir. Bu sırada finansal kayıplar artar.
-Her şekilde bir yedekleme altyapısına ihtiyaç duyar. Yani teypten dönmek düşünüldüğü kadar kolay ve ucuz olmayabilir.

Geleneksel Felaket Kurtarma Merkezi (DR)

-Yedeklerinize saldırırlar yani herseyi bir anda kaybedebilirsiniz.
-Replikasyon probleme bir çözüm değil, katalizör olabilir.

Retention Lock (Ana Veri Merkezinde)

-Ana Veri Merkezine yapılan ransomware saldırılarında retention lock'un ne kadar engelleyici olabileceği değerlendirilmesi gereken bir konudur.
-Her sistem saldırı altındadır.

Hava Boşluğu (Air Gap) Olmayan / Tamamen Korunmamış Ortamlara dair problemler

Koruma Metodolojisi	Senaryo ve Problem
Yedekler	**Ransomware:** Yedek verinizi veya kataloğu siler, şifreler veya değiştirir. Yedekleme sunucusunu devre dışı bırakır. **İç Düşman:** Yedekleri siler.
Snapler	**Ransomware:** RPO kısadır, kendini gizlemiş saldırgan kodlar problem yaratır. Sunucuları devre dışı bırakır. **İç Düşman:** Snap kopyalarını siler.
“Immutable” or “Hidden” (Gizli kopyalar)	**Ransomware:** Tanıma dikkat etmek lazım. «Gizli kopya» tam olarak nedir? SEC 17a4-(f)(2) benzeri standartlar içerir mi? Üretici garantiyebilir mi? **İç Düşman:** Cok basitçe verileri siler.
Gercek Retention Lock (Yedeklerin değişmemek üzere kilitlenmesi)	**Ransomware:** iyi bir koruma sağlar ama kataloğunda korunması lazım. Hava boşluğu arkasında ve Kasada olmadığı için minimumda olsa güvenlik açıkları oluşturabilir. **İç Düşman:** Retention Lock’ı kapatabilir, Zaman ayarı ile oynayabilir. Admin override varmı?

“Veri Svalbardı” veya İzole Korunak

Kritik Veri Her An Erişilen Şebekeden Ayrı ve İzole Yaşatılıyor.

Siber Kurtarma Analitiği
Cyber Sense Uygulaması

Enhanced Dell EMC PowerProtect Cyber Recovery

Powerful
Support for PowerProtect Data Manager and recovery of backups from Cyber Recovery Vault

Integrated
Enhanced Integration with Index Engines CyberSense for robust data set anomaly detection using ML

Expanded
Validated with OWL Data Diode & Unisys Stealth®

Simple
UI/UX improvements for more efficient workflow orchestration