FİDYECİ YAZILIM NEDİR?

Bulaştıkları sistemlerde dosyalara erişimi engelleyerek kullanıcılardan fidye talep edilmesine olanak sağlayan yazılımlardır.

Uluslararası araştırma ve raporlar, fidye yazılımı saldırılarının küresel ölçekte büyük maddi zararlara yol açtığını ve ciddi tehdit oluşturduğunu ortaya koyuyor.

Yoğun şekilde hedef haline gelen işletmelerin, saldırıları önleme veya gerçekleşen saldırıların etkilerini en aza indirme konularında önemli sorumluluk ve zorunlulukları bulunuyor.

SİBERAY
SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI

@siberayegm

www.siberay.com

EMNİYET GENEL MÜDÜRLÜĞÜ
SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
siber@egm.gov.tr
0 (312) 462 55 00
İncek Mahallesi Boztepe Sokak No:125
Gölbaşı / Ankara

SİBERAY
SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI

FİDYECİ YAZILIM

(RANSOMWARE)

SALDIRILARDAN KORUNMAK İÇİN NELER YAPILMALI?

- Güvenli olmayan bağlantılara asla tıklamayın.
- Kişisel bilgilerinizi paylaşmaktan kaçının.
- Şüpheli e-posta eklerini açmayın.
- Kaynağı bilinmeyen USB belleklerini asla kullanmayın.
- Programlarınızı ve işletim sisteminizi güncel tutun.
- Yalnızca resmi çevrim içi indirme kaynaklarını kullanın.
- Herkese açık Wi-Fi ağlarında VPN hizmetlerini kullanın.
- Düzenli olarak veri yedekleme prosedürlerini uygulayın.

Veri Yedekleme Prosodürleri

Yedeklerinizi ayrı ayrı depolayın.

Yedeklemelerin düzenli olarak test edildiğinden emin olun.

Harici sabit sürücü gibi ağdan erişilemeyen cihazlarda saklayın.

Sistemleri yeniden kurmak için yedek donanımı saklayın.

ŞÜPHELİ BİR DURUMDA NELER YAPILMALI?

Sistemdeki yetkili kullanıcı bilgilerini ve şifrelerini en kısa sürede değiştirin.

Etkilenen sistemi izole edin.

Diğer bilgisayarları ve cihazları ağdan ayırarak kapatın.

Yedeklemelerinizin güvende olduğundan emin olun.