SİBER GÜVENLİK SÖZLÜĞÜ

100 Temel Siber Güvenlik Terimi

Erasmus+ KA210-ADU Projesi
2023-1-TR01-KA210-ADU-000165733

TEHDİTLER - Zararlı Yazılımlar

1. **Virüs** - Bilgisayara bulaşarak dosyalara zarar veren ve kendini kopyalayan zararlı yazılım.
2. **Solucan** - Ağ üzerinden otomatik olarak yayılan, kendini çoğaltan zararlı yazılım türü.
3. **Truva Atı** - Yararlı görünüp arka planda zararlı işlemler yapan gizli yazılım.
4. **Ransomware** - Dosyaları şifreleyip fidye talep eden zararlı yazılım. Fidye yazılımı.
5. **Spyware** - Kullanıcı bilgilerini gizlice toplayan casus yazılım.
6. **Adware** - İstenmeyen reklamlar gösteren ve tarayıcıyı yavaşlatan yazılım.
7. **Rootkit** - Sisteme gizlice yerleşip tam kontrol sağlayan tehlikeli yazılım.
8. **Keylogger** - Klavyede basılan tuşları kaydeden casus yazılım.
9. **Botnet** - Hackerların uzaktan kontrol ettiği virüslü bilgisayarlar ağı.
10. **Malware** - Zararlı yazılım. Virüs, solucan, truva atı gibi tehditlerin genel adı.
11. **Zero-Day** - Henüz yaması olmayan, yeni keşfedilmiş güvenlik açığı.
12. **Exploit** - Güvenlik açıklarından yararlanan saldırı kodu veya tekniği.
13. **Backdoor** - Sisteme gizli giriş sağlayan arka kapı erişimi.
14. **RAT** - Uzaktan erişim truva atı. Bilgisayarın uzaktan kontrolünü sağlar.
15. **Cryptojacking** - Başkalarının bilgisayarını kripto para madenciliği için kullanan saldırı.
16. **Scareware** - Sahte güvenlik uyarılarıyla kullanıcıyı korkutup para isteyen yazılım.
17. **Logic Bomb** - Belirli koşullar oluştuğunda aktifleşen zararlı kod.
18. **Fileless Malware** - Dosya bırakmadan bellekte çalışan tespit edilmesi zor zararlı.
19. **Dropper** - Sisteme başka zararlı yazılımları indirip yükleyen program.

20 **Wiper** - Verileri kalıcı olarak silen, kurtarılamaz hale getiren zararlı yazılım.

SALDIRILAR - Siber Saldırı Teknikleri

21 **Phishing** - Sahte e-posta veya sitelerle kişisel bilgi çalma saldırısı. Oltalama.

22 **Smishing** - SMS yoluyla yapılan oltalama saldırısı.

23 **Vishing** - Telefon aramasıyla yapılan sesli oltalama saldırısı.

24 **Spear Phishing** - Belirli kişi veya kurumu hedef alan özelleştirilmiş oltalama.

25 **Whaling** - Üst düzey yöneticileri hedef alan oltalama saldırısı.

26 **DDoS** - Çok sayıda kaynaktan yapılan hizmet engelleme saldırısı.

27 **DoS** - Sistemi aşırı yükleyerek hizmet dışı bırakan saldırı.

28 **Man-in-the-Middle** - İki taraf arasındaki iletişimi gizlice dinleyen saldırı. Ortadaki adam.

29 **SQL Injection** - Veritabanına zararlı SQL kodları enjekte eden saldırı.

30 **XSS** - Web sitelerine zararlı kod yerleştiren çapraz site saldırısı.

31 **Brute Force** - Tüm olası şifre kombinasyonlarını deneyen kaba kuvvet saldırısı.

32 **Dictionary Attack** - Yaygın şifreleri listeden deneyen sözlük saldırısı.

33 **Credential Stuffing** - Çalınan kimlik bilgilerini farklı sitelerde deneyen saldırı.

34 **Session Hijacking** - Aktif oturumu ele geçirerek yetkisiz erişim sağlama.

35 **DNS Spoofing** - DNS kayıtlarını değiştirerek sahte sitelere yönlendirme.

36 **ARP Spoofing** - Yerel ağda trafiği yönlendirmek için ARP tablolarını manipüle etme.

37 **Pharming** - DNS manipülasyonuyla kullanıcıları sahte sitelere yönlendirme.

38 **Social Engineering** - İnsan psikolojisini kullanarak bilgi elde etme. Sosyal mühendislik.

39 **Baiting** - Ücretsiz bir şey vaadiyle kurbanı tuzağa düşürme saldırısı.

40 **Pretexting** - Sahte senaryo oluşturarak güven kazanıp bilgi alma tekniği.

KORUMA - Güvenlik Önlemleri

41 **Antivirus** - Zararlı yazılımları tespit edip temizleyen güvenlik programı.

42 **Firewall** - Ağ trafiğini kontrol eden güvenlik duvarı.

43 **2FA** - İki faktörlü kimlik doğrulama. Ekstra güvenlik katmanı.

44 **MFA** - Çok faktörlü kimlik doğrulama. Birden fazla doğrulama yöntemi.

45 **Şifreleme** - Verileri okunamaz hale getiren koruma yöntemi. Encryption.

46 **SSL/TLS** - İnternet trafiğini şifreleyen güvenli bağlantı protokolü.

47 **HTTPS** - Güvenli web bağlantısı. Şifreli HTTP protokolü.

48 **VPN** - İnternet trafiğini şifreleyip gizleyen sanal özel ağ.

49 **Yedekleme** - Verilerin kopyasını alma. Veri kaybına karşı koruma. Backup.

50 **Güncelleme** - Yazılımların güncel tutulması. Güvenlik açıklarını kapatır.

51 **Parola Yöneticisi** - Şifreleri güvenle saklayan ve yöneten uygulama.

52 **Sandbox** - Şüpheli dosyaları güvenli ortamda test eden izole alan.

53 **IDS** - Şüpheli aktiviteleri tespit eden saldırı tespit sistemi.

54 **IPS** - Saldırıları tespit edip engelleyen saldırı önleme sistemi.

55 **WAF** - Web uygulamalarını koruyan web uygulama güvenlik duvarı.

56 **Endpoint Security** - Bilgisayar ve cihazları koruyan uç nokta güvenliği.

57 **Zero Trust** - Hiçbir şeye güvenme, her şeyi doğrula güvenlik yaklaşımı.

58 **Yama** - Yazılım hatalarını ve açıklarını düzelten güncelleme. Patch.

59 **Beyaz Liste** - Yalnızca izin verilen uygulamaların çalışmasına izin verme.

60 **Kara Liste** - Bilinen zararlı sitelerin veya yazılımların engellenmesi.

ARAÇLAR - Teknoloji ve Altyapı

61 **IP Adresi** - İnternetteki cihazların benzersiz kimlik numarası.

62 **MAC Adresi** - Ağ kartının benzersiz fiziksel adresi.

63 **DNS** - Alan adlarını IP adreslerine çeviren sistem.

64 **Router** - Ağ trafiğini yönlendiren cihaz. Yönlendirici.

65 **Proxy** - İnternet trafiğini yönlendiren aracı sunucu.

66 **Port** - Ağ iletişiminde kullanılan sanal bağlantı noktası.

67 **Protokol** - Cihazlar arası iletişim kuralları. HTTP, FTP, TCP gibi.

68 **Cookie** - Web sitelerinin tarayıcıda sakladığı küçük veri dosyaları.

69 **Cache** - Hızlı erişim için geçici olarak saklanan veriler. Önbellek.

70 **Token** - Kimlik doğrulama için kullanılan dijital anahtar.

71 **Hash** - Veriden üretilen benzersiz sabit uzunlukta değer. Özet.

72 **API** - Yazılımların birbiriyle iletişim kurmasını sağlayan arayüz.

73 **Bulut** - İnternet üzerinden erişilen uzak sunucu hizmetleri. Cloud.

74 **Metadata** - Veri hakkında bilgi veren üst veri. Dosya bilgileri gibi.

75 **Bandwidth** - Ağ bağlantısının veri taşıma kapasitesi. Bant genişliği.

76 **Latency** - Veri iletimindeki gecikme süresi.

77 **Ping** - Ağ bağlantısını test eden komut.

78 **Traceroute** - Veri paketinin izlediği yolu gösteren araç.

79 **Tor** - Anonim internet gezintisi sağlayan ağ.

80 **Dark Web** - Özel yazılımlarla erişilen gizli internet alanı.

KAVRAMLAR - Temel Bilgiler

81 **Siber Güvenlik** - Dijital sistemleri ve verileri koruma bilimi.

82 **Veri İhlali** - Yetkisiz kişilerin hassas verilere erişmesi. Data breach.

83 **Kimlik Hırsızlığı** - Başkasının kimlik bilgilerini çalıp kullanma.

84 **Spam** - İstenmeyen toplu e-posta veya mesajlar.

85 **CAPTCHA** - İnsan ve bot ayırt eden doğrulama testi.

86 **Gizlilik** - Kişisel bilgilerin korunması. Privacy.

87 **Anonim** - Kimliği gizli, takip edilemeyen. Anonymous.

88 **Açık Kaynak** - Kaynak kodu herkese açık olan yazılım. Open source.

89 **Penetrasyon Testi** - Sistemin güvenliğini test eden simüle saldırı. Pentest.

90 **Zafiyet** - Sistemdeki güvenlik açığı veya zayıflık. Vulnerability.

91 **Risk** - Olası tehdit ve zararın değerlendirilmesi.

92 **Compliance** - Güvenlik standartlarına ve yasalara uyumluluk.

93 **GDPR** - Avrupa Birliği genel veri koruma yönetmeliği.

94 **KVKK** - Kişisel Verilerin Korunması Kanunu. Türkiye'nin veri koruma yasası.

95 **Siber Saldırı** - Dijital sistemlere yapılan kasıtlı zarar verme girişimi.

96 **Hacker** - Bilgisayar sistemlerine sızan kişi. Etik veya kötü niyetli olabilir.

97 **White Hat** - Etik hacker. İzinli güvenlik testi yapan uzman.

98 **Black Hat** - Kötü niyetli hacker. Yasadışı sızma yapan kişi.

99 **Bug Bounty** - Güvenlik açığı bulan kişilere ödül veren program.

100 **Dijital Ayak İzi** - İnternette bırakılan izler ve veriler.

Bu yayının üretilmesi için Avrupa Komisyonu'nun desteği, yalnızca yazarların görüşlerini yansıtan içeriklerin onaylandığı anlamına gelmez ve Komisyon, burada yer alan bilgilerin herhangi bir şekilde kullanılmasından sorumlu tutulamaz.