

IT DÜNYASI KIBERTƏHLÜKƏSİZLİK



KIBERTƏHLÜKƏSİZLIYƏ GIRIŞ

- Kibertəhlükəsizlik nədir?
- Kibertəhlükəsizlik, kompüter sistemlərinin, şəbəkələrin, proqramların və məlumatların kibertəhlükələrdən qorunması prosesidir. Kibertəhlükələr, məlumat oğurluğu, sistemlərə zərər vurma, məlumatların pozulması və ya ələ keçirilməsi, zərərli proqramların yayılması kimi hər hansı bir pis niyyətli fəaliyyətləri əhatə edir. Kibertəhlükəsizlik, bu cür təhdidlərə qarşı mübarizə aparmaq və məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını qorumaq məqsədi daşıyır.

KIBERTƏHLÜKƏLƏR

- **Ən geniş yayılmış kibertəhlükələr**
- Zərərli proqramlar (viruslar, troyanlar, spyware)
- Fişinq və sosial mühəndislik hücumları
- DDoS hücumları

ŞƏXSİ MƏLUMATLARIN QORUNMASI

- Məlumatların qorunması üçün əsas tədbirlər
- Güclü Parollar, Məlumatların Şifrələnməsi, Firewall və Antivirus, Müntəzəm Yeniləmələr, Yedəkləmə Bulud istifadəsi, Təhlükəsizlik Təlimləri, Məhdud Giriş, Təhlükəsizlik Auditi və Monitoring, İstifadə edilməyən Məlumatların Silinməsi

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ

- Şəbəkə təhlükəsizliyi nədir?

- Şəbəkə təhlükəsizliyi, bir kompüter şəbəkəsini icazəsiz girişlərdən, sui-istifadə, dəyişiklik və ya xidmətlərin kəsilməsindən qorumaq məqsədilə tətbiq olunan qaydalar və tədbirlər toplusudur. Şəbəkə təhlükəsizliyinin əsas məqsədi məlumatların və resursların qorunmasını təmin etməkdir.

ŞIFRLƏMƏ VƏ AVTORİZASIYA

- Şifrləmənin əsasları
- İdentifikasiya və avtorizasiya metodları

İdentifikasiya: İlk olaraq istifadəçi və ya sistem öz şəxsiyyətini təsdiq edir. Bu adətən istifadəçi adı və parol ilə həyata keçirilir.

Avtorizasiya: Autentifikasiya uğurlu olduqdan sonra sistem istifadəçinin hansı resurslara və funksiyalara giriş icazəsinin olduğunu müəyyən edir və bu icazələri tətbiq edir.

QLOBAL KIBERTƏHLÜKƏSİZLİK TRENDLƏRİ

- Mövcud və gələcək trendlər
- Kibertəhlükəsizliyin gələcəyi
- Süni intellekt (AI) və maşın öyrənməsi kibertəhlükəsizlikdə böyük rol oynayır. Bu texnologiyalar anomaliyaları aşkar etmək, təhlükəsizlik boşluqlarını müəyyənləşdirmək və hücumları əvvəlcədən təxmin etmək üçün istifadə olunur. Eyni zamanda, kiber cinayətkarlar da bu texnologiyalardan faydalanaraq daha mürəkkəb hücumlar həyata keçirirlər.
- Dövlətlər arasında kiber hibrid müharibənin artması müşahidə olunur. Kiber hücumlar hərbi və siyasi məqsədlər üçün istifadə olunur və bu, qlobal təhlükəsizlik üçün ciddi təhdidlər yaradır.

KIBERTƏHLÜKƏSİZLIK STANDARTLARI VƏ QANUNVERICILIK

- Yerli qanunvericilik və tənzimləmələr
- Kompüter məlumatlarına qanunsuz daxil olma, Kompüter məlumatlarının məhv edilməsi və ya dəyişdirilməsi, Zərərli proqramların yayılması, Şəxsi məlumatların qanunsuz toplanması və yayılması, Elektron məlumatların saxtalaşdırılması.
- Bu qanunvericilik aktları kibertəhlükəsizlik sahəsində cinayət məsuliyyətini müəyyən edir və bu cür cinayətlərin qarşısını almaq üçün hüquqi baza yaradır. Azərbaycan qanunlarına əsasən, kibercinayətlər ciddi hüquqi nəticələr doğura bilər və pozucular cinayət məsuliyyətinə cəlb edilə bilərlər.

KIBERTƏHLÜKƏSİZLİK ÜZRƏ TƏHSİL

- Azərbaycanda Kibertəhlükəsizlik üzrə təhsil proqramları
- Azərbaycan Dövlət Neft və Sənaye Universiteti İnformasiya Təhlükəsizliyi: Bu proqram tələbələrə informasiya təhlükəsizliyi sahəsində nəzəri və praktiki biliklər verir
- Bakı Mühəndislik Universiteti Kompüter Elmləri və İnformasiya Texnologiyaları Fakültəsi: Bu fakültədə kibertəhlükəsizlik üzrə ixtisaslaşma imkanları mövcuddur.
- Azərbaycan Texniki Universiteti İnformasiya və Kommunikasiya Texnologiyaları Fakültəsi: İnformasiya təhlükəsizliyi sahəsində müxtəlif kurslar təklif edir

SUAL VƏ CAVAB

- Auditoriya ilə interaktiv müzakirə

BONUS SLAYD 😊



Hackers

- **White Hat Hackers**
- **Black Hat Hackers**
- **Gray Hat Hackers**