MEB - Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü Siber Güvenliğe Giriş Eğitimi 3.DERS 08.04.2020

Introduction to Cybersecurity v2.1

KVKK!

Yayınlanma Tarihi: 07.04.2020

Uzaktan Eğitim Platformları Hakkında Kamuoyu Duyurusu

Uzaktan eğitim platformlarında, öğrencilerin ad ve soyadları gibi kişisel verileri ile ses ve görüntü gibi biyometrik veri kapsamında değerlendirilebilecek bazı özel nitelikli kişisel verilerinin işlendiği görülmektedir.

6698 sayılı Kişisel Verilerin Korunması Kanununun 5 inci maddesinde kişisel verilerin işlenme şartları, 6 ncı maddesinde ise biyometrik verilerin dâhil olduğu özel nitelikli kişisel verilerin işlenme şartları belirlenmiştir. Bu noktada, kişisel verilerin Kanunun 5 inci ve/veya 6 ncı maddesinde belirtilen şartlara uygun olarak işlenmesi gerekmektedir.

Bununla birlikte uzaktan eğitim amacıyla kullanılan yazılımların birçoğunun bulut hizmet sağlayıcılar aracılığıyla hizmet verdiği ve bu yazılımlara ait veri merkezlerinin çoğunlukla yurt dışında olduğu gözlemlenmektedir. Veri merkezleri yurtdışında olan platformların kullanılması durumunda yurtdışına veri aktarımı söz konusu olacağından, Kişisel Verilerin Korunması Kanununun 9 uncu maddesinde belirtilen şartlara uygun olmayan aktarımların Kanunun ihlali anlamına gelebileceği unutulmamalıdır.

Bu bağlamda, uzaktan eğitim hizmeti amacıyla kullanılan bu platformların gerekli veri güvenlik tedbirlerini alıp almadıkları ile ilgili Kişisel Verileri Koruma Kurulu tarafından hazırlanan “Kişisel Veri Güvenliği Rehberi (İdari ve Teknik Tedbirler) ile Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" Kararı göz önünde bulundurulmalıdır.

Kamuoyuna saygıyla duyurulur.

https://www.kvkk.gov.tr/Icerik/6723/Uzaktan-Egitim-Platformlari-Hakkinda-Kamuoyu-Duyurusu

01.04.2020 – Bölüm 1: Siber Güvenlik Gereksinimi
2.Ders Öğrendiklerimiz! Farkındalıklarımız!

Güvenlik açığı !ZAFİYET (vulnerability)!

!Saldırı (Attack)!

İstismar (exploit) – Kali-Metasploit

Yazılım – Donanım Güvenlik Açıkları

Kötü Amaçlı Yazılımın Belirtileri!

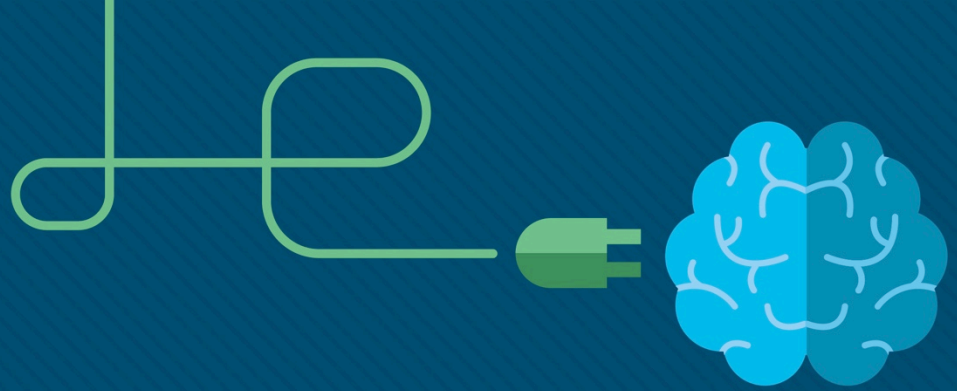
Sosyal Mühendislik - https://bilgiguvende.com/ Bi bakın derim!

Kaba kuvvet saldırıları (Brute-force attacks) ve kullanılan araçlar!

YAZILIMIN GÜNCEL OLSUN!!

Phishing (Oltalama) - **Spear phishing** (**Hedef Odaklı** Oltalama)

OWASP!



Bölüm 3: Verilerinizi ve Gizliliğinizi Koruma

Introduction to Cybersecurity v2.1

Bölüm 3 - Bölümler ve Hedefler

3.1 Verilerinizi Koruma

- Cihazları tehditlerden nasıl koruyacağınızı açıklayın.
  - Cihazlarınızı ve ağınızı nasıl koruyacağınızı açıklayın.
  - Veri bakımı için güvenli prosedürleri açıklayın.

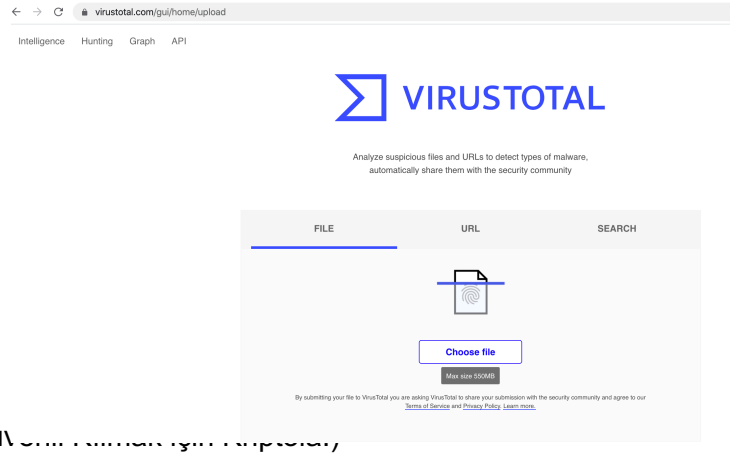
3.2 Çevrimiçi Gizliliğinizi Koruma

- Gizliliğinizi nasıl koruyacağınızı açıklayın.
  - Güçlü kimlik doğrulama yöntemlerini açıklayın.
  - Güvenli çevrimiçi davranışları açıklayın.

3.1 Verilerinizi Koruma

Bilgi İşlem Cihazlarınızı Koruma

- Güvenlik Duvarını Açık Tutun
  - Verilerinize veya bilgi işlem cihazlarınıza yetkisiz erişimi önleyin!
  - Güvenlik duvarını güncel tutun!
- Anti virüs ve Casus Yazılım Önleme Yazılımları kullanın
  - Verilerinize veya bilgi işlem cihazlarınıza yetkisiz erişimi önleyin
  - Yalnızca güvenilir web sitelerinden yazılım indirin
  - Yazılımı güncel tutun
- İşletim Sisteminizi ve Tarayıcınızı Yönetin
  - Güvenlik ayarlarını orta veya daha yüksek bir düzeye getirin
  - Bilgisayarınızın işletim sistemini ve tarayıcısını güncelleyin
  - En son yazılım yamalarını ve güvenlik güncellemelerini indirin ve yükleyin
- Tüm Cihazlarınızı Koruyun
  - Parola koruması
  - Verileri şifreleme – (Windows: Klasör – Sağ Click – Özellikler-Gelişmiş-Veriyi Gü[illegible])
  - Sadece gerekli bilgileri saklayın!
  - IoT cihazları



Kablosuz Ağları Güvenli Bir Şekilde Kullanın!

- Ev Kablosuz Ağı
  - Wi-Fi yönlendiricinizde önceden ayarlanmış SSID ve varsayılan yönetim şifresini değiştirin.
  - SSID yayınını devre dışı bırakın
  - WPA2 şifreleme özelliğini kullanın
  - WPA2 protokolü güvenlik açığına dikkat edin - **KRACK**
    - Saldırganın kablosuz yönlendirici ve istemciler arasındaki şifrelemeyi kırmasına izin verir
- Herkese açık Wi-Fi noktalarını kullanırken dikkatli olun
  - Hassas bilgilere erişmekten veya göndermekten kaçının
  - VPN tünelinin kullanılması gizli dinlemeyi önleyebilir
- Kullanmadığınızda Bluetooth'u kapatın

Parola ve Şifre arasındaki fark ?

Parola!

Bir sisteme girmemiz için belirlediğimiz harflerden, rakamlardan ve özel karakterlerden oluşan sözcüktür, metindir.
Sisteme girme iznimizdir.
İnternet sitelerindeki kullanıcı girişlerinde kullandığımız paroladır,
Kablosuz internete erişmemiz için girmemiz gereken paroladır,

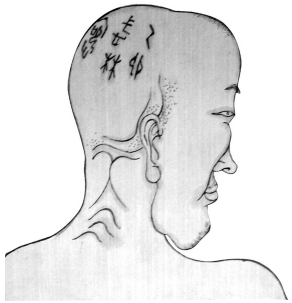
Şifre değildir. !

Şifre

Bir metni, bir parolayı **bir algoritmaya göre** anlamsız hale getirme işlemleri sonrasında yaratılan veridir.

Belirli bir anahtar sayesinde çeşitli matematiksel işlemlerden geçirilerek ilk bakışta anlamsız ve anahtar sayesinde çözülen ifadelere denir.

İlk Şifreleme!

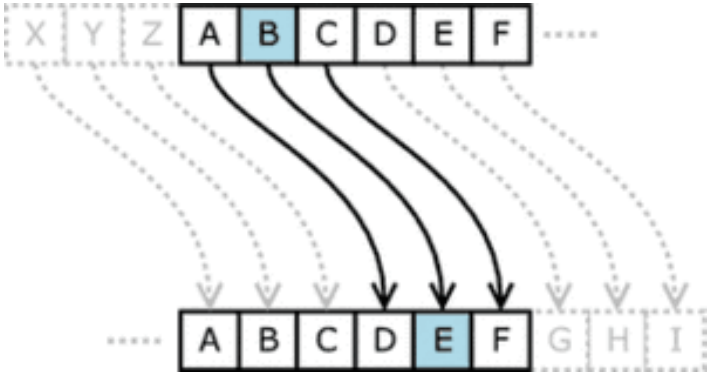


MÖ 500'ler Antik Yunan kafa derisindeki mesaj!

En eski zamanlardan beri insanlar iletişim kurarken mesajlarını gizleme ihtiyacı duymuşlardır.

Çok daha ilkel şifreleme yöntemleri kullanan bu dönemler, mekaniğin ve elektronik cihazların hayatımıza girmesiyle epey bir yol almıştır.

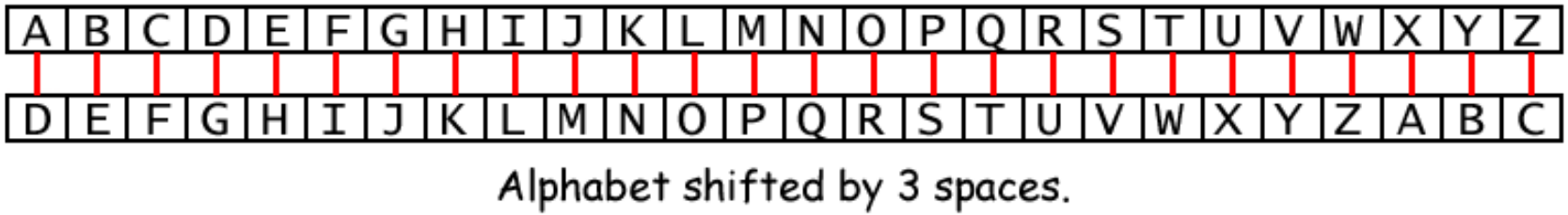
Saç kazıtma bunların en başında gelir.
Sezar algoritması matematiksel olarak ilk örneklerdendir.



Sezar Şifreleme

Örnek;

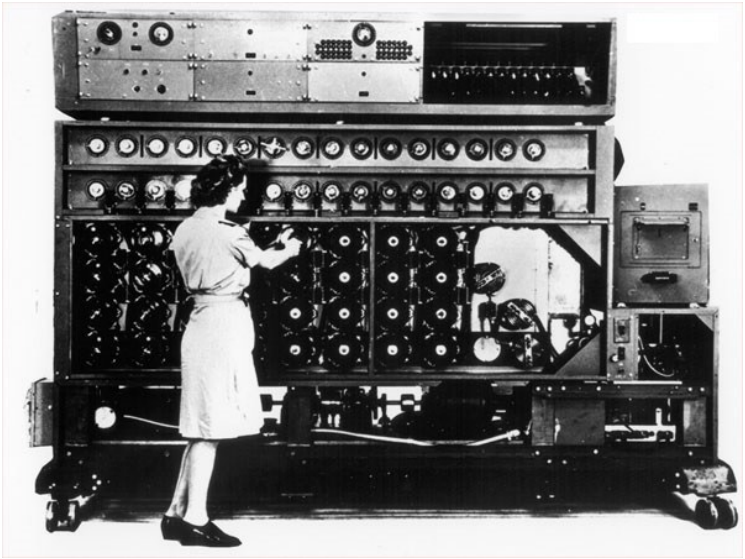
Ahmet = ?
Siber = ?

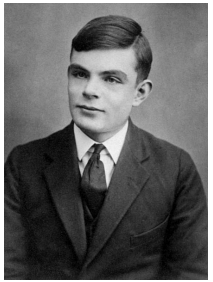


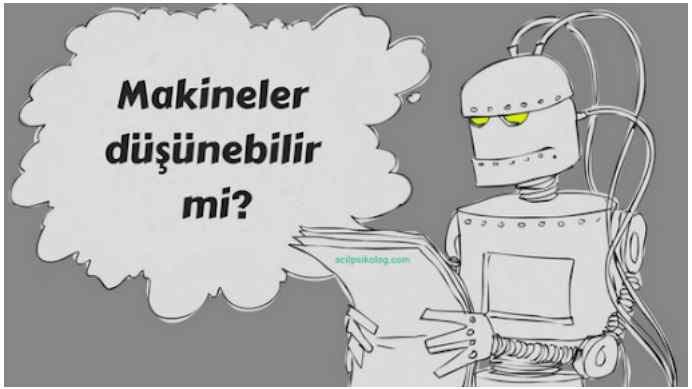
Alphabet shifted by 3 spaces.

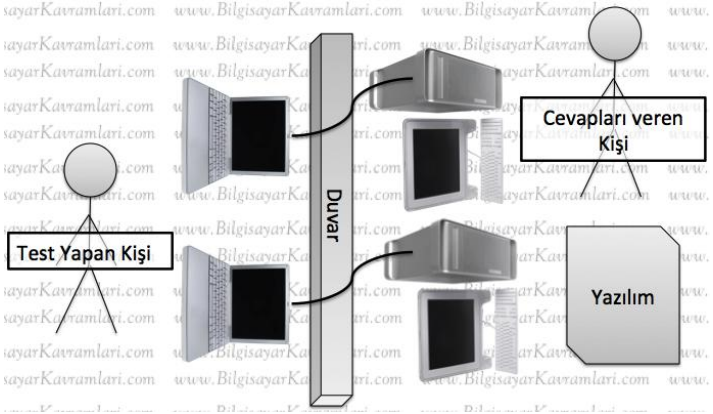
ENIGMA!

ALAN TURING









Geliştirmiş olduğu Turing testi ile makinelerin ve bilgisayarların düşünme yetisine sahip olup olamayacakları konusunda bir kriter öne sürmüştür.
Kaynak:
https://tr.wikipedia.org/wiki/Alan_Turing

BİRAZ DAHA KAVRAM!

- **Kriptoloji:** Kriptoloji, bir şifre ve şifreleme **bilimidir**. Çeşitli bilgilerin, belli bir sisteme göre şifrelenmesi, bu mesajların güvenlikli bir ortamda iletilmesi ve iletilen mesajın orijinal hale getirilmesi ile uğraşır. Kriptoloji, genel olarak askerî kurumlarda ve aynı zamanda internet dahilindeki kişiler arası haberleşmelerde kullanılmaktadır.

- **Encryption/Şifreleme:** Bir verinin sadece gizli anahtarı bilen yetkili kişilerce okunabilmesi amaçlı gerçekleştirilen **format değişikliği** olarak bilinir.

- RSA ve AES, en sık kullanılan şifreleme algoritmalarındandır.

Her Çevrimiçi Hesap için Benzersiz Parolalar Kullanın

- Suçluların çalınan kimlik bilgilerini kullanarak tüm çevrimiçi hesaplarınıza erişmesini önler
- Şifreleri hatırlamaya yardımcı olması için şifre yöneticilerini kullanın
- İyi bir şifre seçmek için ipuçları:
  - Sözlük kelimelerini veya adlarını hiçbir dilde kullanmayın
  - Sözlük kelimelerinin ortak yazım hatalarını kullanmayın
  - Bilgisayar adları veya hesap adları kullanmayın
  - Mümkünse **! @ # $ % ^ & * ( )** gibi özel karakterler kullanın
  - On veya daha fazla karakterden oluşan bir şifre kullanın

OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

http://password-checker.online-domain-tools.com/

Parola yerine Çoklu Kelime (Passphrase) Kullanın

- İyi bir Çoklu Kelime Parolası seçmeyle ilgili ipuçları:
  - **Size** anlamlı bir ifade seçin
  - **! @ # $ % ^ & * ( )** gibi özel karakterler ekleyin
  - Ne kadar uzunsa o kadar iyi
  - Yaygın veya ünlü ifadelerden kaçının, örneğin: popüler bir şarkının sözleri
- Yeni NIST yönergelerinin özeti:
  - Minimum 8 karakter uzunluğunda, ancak 64 karakterden fazla olmamalıdır
  - Parolanız abc123 gibi yaygın, kolayca tahmin edilen harflerden oluşmamalıdır
  - Küçük harf ve büyük harf ve sayı eklemek gibi kompozisyon kuralları yoktur
  - Paylaşılan gizli sorulardan bilgi, pazarlama verileri, işlem geçmişi gibi bilgiye dayalı kimlik doğrulama yok
  - Yazarken kullanıcının şifreyi görmesine izin vererek yazma doğruluğunu artırın
  - Tüm yazdırma karakterlerine ve boşluklara izin verilir
  - Şifre ipucu yok
  - Periyodik veya rastgele şifre süresinin dolması yok

OK	Thisismypassphrase.
Good	Acatthatlovesdogs.
Better	Acat th@tlov3sd0gs.

Parolalar ? Zaten önemli olduğunu biliyoruz…

• Doğru. Ama Hacker'ların içeri girmek için hala en SIK kullandığı yöntem!

• Kullanıcı düzeyinde erişim genellikle yetki yükseltmesine yol açar

- Arabellek taşmaları
- Uygulama hataları
- Yapılandırma dosyaları parolaları
- SNMP Topluluk Dizisi

Erişim Sağlama (Gain Access)

“Parola diş fırçanız gibidir. Başkasının kullanmasına izin vermeyin, ve altı ayda bir yenileyin.”

“Treat your password like your toothbrush. Don‟t let anybody else use it, and get a new one every six months.”

Clifford Stoll
Author

One Of The 32 Million With A RockYou Account? You May Want To Change All Your Passwords. Like Now.

Million With A RockYou lay Want To Change All Your Passwords. Like Now.

by **MG Siegler** on Dec 14, 2009 **104 Comments** **468** retweet Share 269 Buzz it

It's no secret that most people use the same password over and over again for most of the services they sign up for. While it's obviously convenient, this becomes a major problem if one of those services is compromised. And that looks to be the case with **RockYou** , the social network app maker.

Over the weekend, the security firm **Imperva** issued a **warning** to RockYou that there was a serious SQL Injection flaw in their database. Such a flaw could grant hackers access to the the service's entire list of user names and passwords in the database, they warned. Imperva said that after it notified RockYou about the flaw, it was apparently fixed over the weekend. But that's not before at least one hacker **gained access** to what they claim is *all* of the 32 million accounts. 32,603,388 to be exact. The best part? The database included a full list of unprotected plain text passwords. And email addresses. Wow.

Parolar….

Cisco Networking Academy

En Çok Kullanılan 10 rockyou.com Parolası… 32 milyon hesapta

1. 123456
2. 12345
3. 123456789
4. password
5. iloveyou
6. princess
7. 1234567
8. rockyou
9. 12345678
10. abc123

Lab – Güçlü Parolalar Oluşturun ve Saklayın

Networking Academy

Lab – Create and Store Strong Passwords

Objectives

Understand the concepts behind a strong password.

Part 1: Explore the concepts behind creating a strong password.

Part 2: Explore the concepts behind securely storing your passwords?

Background / Scenario

Passwords are widely used to enforce access to resources. Attackers will use many techniques to learn users' passwords and gain unauthorized access to a resource or data.

To better protect yourself, it is important to understand what makes a strong password and how to store it securely.

Required Resources

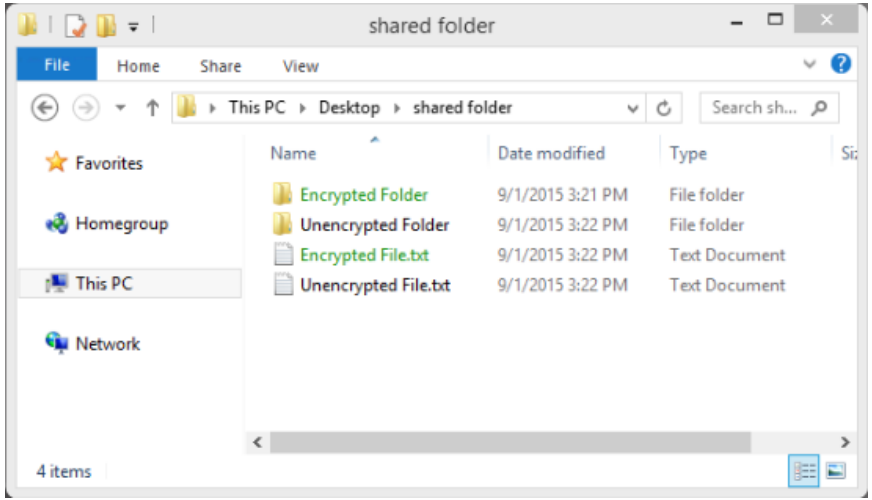
- PC or mobile device with Internet access

Part 1: Creating a Strong Password

Strong passwords have four main requirements listed in order of importance:

Verilerinizi Şifreleyin

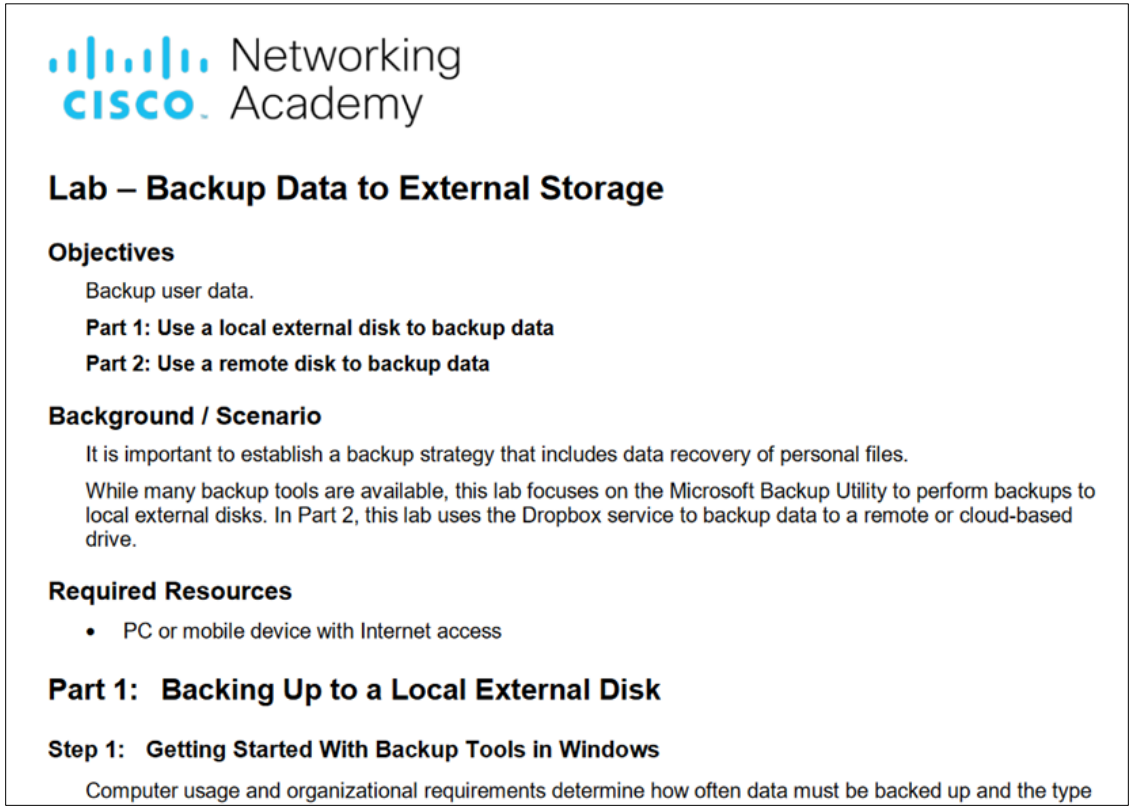
- Şifrelenmiş veriler yalnızca gizli anahtar veya parola ile okunabilir
- Yetkisiz kullanıcıların içeriği okumasını önleyin!
- Şifreleme (encryption) nedir?
  - bilgileri yetkisiz bir tarafın okuyamayacağı bir forma dönüştürme işlemi



Verilerinizi Yedekleyin

- Yeri doldurulamaz verilerin kaybını önler
- Veriler için ek depolama alanı ihtiyacı oluşur
- Verileri yedekleme konumuna düzenli ve otomatik olarak kopyalayın
- Yerel Yedekleme
  - NAS, harici sabit sürücü, CD'ler / DVD'ler, parmak sürücüleri (USB) veya kasetler
  - Tam kontrol sağlar, maliyet ve bakım sorumlusu siz olursunuz
- AWS gibi Bulut Depolama Hizmeti
  - Hesabınıza erişiminiz olduğu sürece yedeklemeye erişim
  - yedeklenen veriler için daha seçici olunması gerekebilir

Lab – Verileri Harici Depolama Alanına Yedekleyin



Networking Academy

Lab – Backup Data to External Storage

Objectives

Backup user data.

Part 1: Use a local external disk to backup data

Part 2: Use a remote disk to backup data

Background / Scenario

It is important to establish a backup strategy that includes data recovery of personal files.

While many backup tools are available, this lab focuses on the Microsoft Backup Utility to perform backups to local external disks. In Part 2, this lab uses the Dropbox service to backup data to a remote or cloud-based drive.

Required Resources

- PC or mobile device with Internet access

Part 1: Backing Up to a Local External Disk

Step 1: Getting Started With Backup Tools in Windows

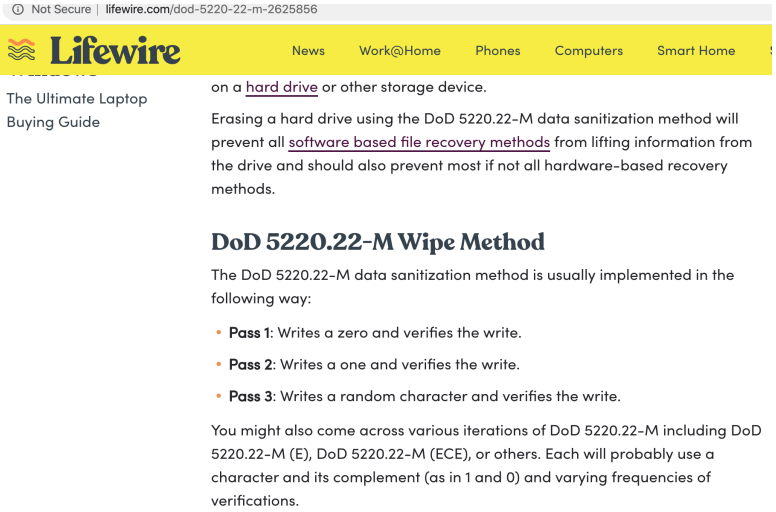
Computer usage and organizational requirements determine how often data must be backed up and the type

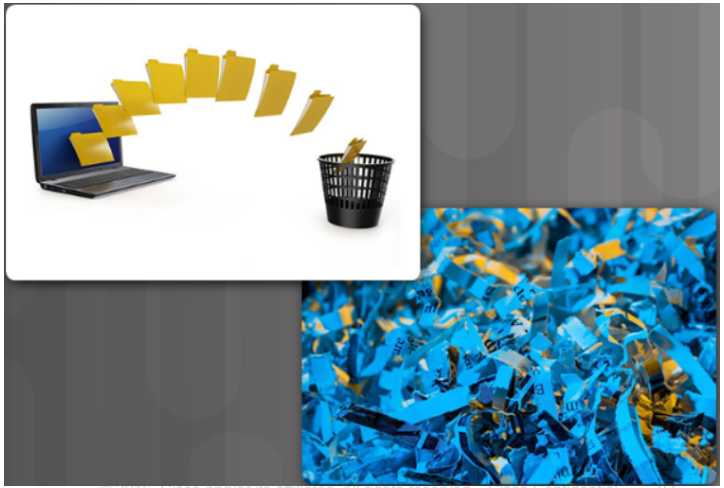
Veri bakımı

Verilerinizi Kalıcı Olarak Silme

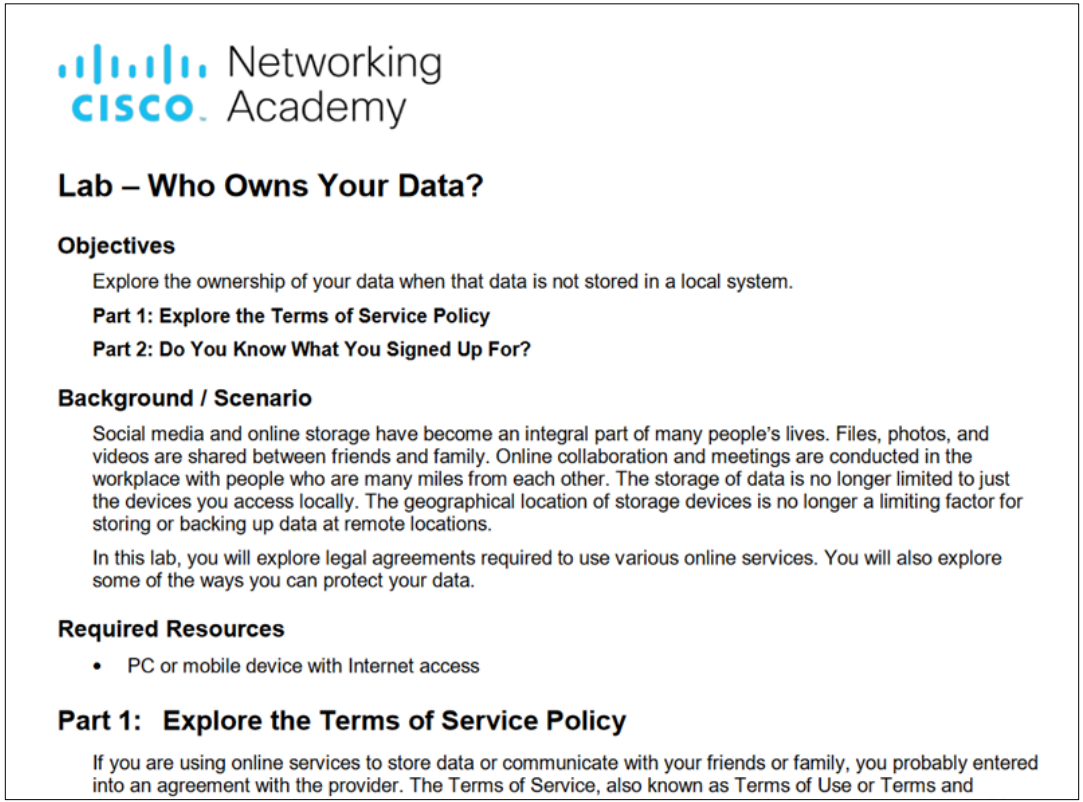
- Kalıcı olarak silmek için mevcut araçları kullanın: Örneğin, **SDelete** ve **Çöp Kutusunu Boşalt**
- Verilerin kurtarılamaz olduğundan emin olmak için depolama cihazını imha edin
- Çevrimiçi sürümleri silin

https://www.lifewire.com/free-file-shredder-software-programs-2619149





Lab – Verilerinizin Sahibi Kim



Networking Academy

Lab – Who Owns Your Data?

Objectives

Explore the ownership of your data when that data is not stored in a local system.

Part 1: Explore the Terms of Service Policy

Part 2: Do You Know What You Signed Up For?

Background / Scenario

Social media and online storage have become an integral part of many people's lives. Files, photos, and videos are shared between friends and family. Online collaboration and meetings are conducted in the workplace with people who are many miles from each other. The storage of data is no longer limited to just the devices you access locally. The geographical location of storage devices is no longer a limiting factor for storing or backing up data at remote locations.

In this lab, you will explore legal agreements required to use various online services. You will also explore some of the ways you can protect your data.

Required Resources

- PC or mobile device with Internet access

Part 1: Explore the Terms of Service Policy

If you are using online services to store data or communicate with your friends or family, you probably entered into an agreement with the provider. The Terms of Service, also known as Terms of Use or Terms and

3.2 Çevrimiçi Gizliliğinizi Koruma

İki Faktörlü Kimlik Doğrulama

- Popüler çevrimiçi hizmetler iki faktörlü kimlik doğrulama kullanır
- Erişim için Kullanıcı Adı / parola veya PIN ve ikinci bir belirteç (token) gerekir:
  - **Fiziksel Nesne** - kredi kartı, ATM kartı, telefon veya fob
  - **Biometrik Tarama** - parmak izi, avuç içi baskısı, yüz veya ses tanıma

Çok Fazla Bilgi mi Paylaşıyorsunuz?

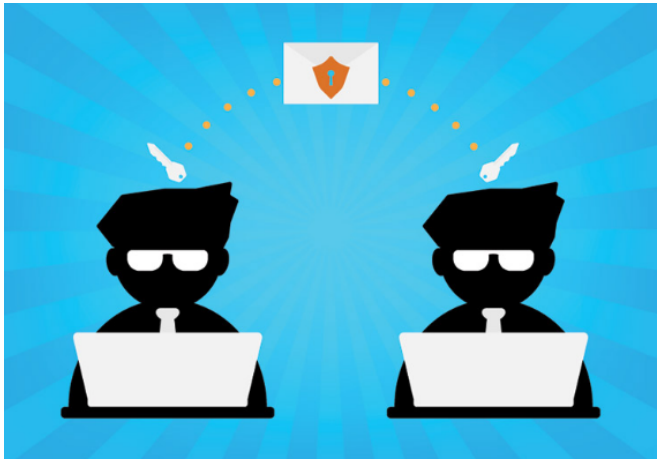
Sosyal Medyada Çok Fazla Paylaşmayın

- Sosyal medyada mümkün olduğunca az bilgi paylaşın
- Aşağıdaki gibi bilgileri paylaşmayın:
  - Doğum günü
  - E-posta Adresi
  - Telefon Numarası
- Sosyal medya **ayarlarınızı** kontrol edin!

Çok Fazla Bilgi mi Paylaşıyorsunuz?

E-posta ve Web Tarayıcı Gizliliği

- E-posta, kartpostal göndermek gibidir.
- E-postanın kopyaları erişimi olan herkes tarafından okunabilir.
- E-posta farklı sunucular arasında aktarılır.
- web tarayıcıyının gizli modunu kullanmak, başkalarının çevrimiçi etkinlikleriniz hakkında bilgi toplamasını engelleyebilir.
- Gizli Mod desteği olan popüler tarayıcılar
  - **Microsoft Internet Explorer**: **InPrivate**
  - **Google Chrome**: **Incognito**
  - **Mozilla Firefox**: **Private tab / private window**
  - **Safari**: **Private: Private browsing**



Lab – Kendi Riskli Çevrimiçi Davranışınızı Keşfedin

Networking Academy

Lab – Discover Your Own Risky Online Behavior

Objectives

Explore actions performed online that may compromise your safety or privacy.

Background / Scenario

The Internet is a hostile environment, and you must be vigilant to ensure your data is not compromised. Attackers are creative and will attempt many different techniques to trick users. This lab helps you identify risky online behavior and provide tips on how to become safer online.

Part 1: Explore the Terms of Service Policy

Answer the questions below with honesty and take note of how many points each answer gives you. Add all points to a total score and move on to Part 2 for an analysis of your online behavior.

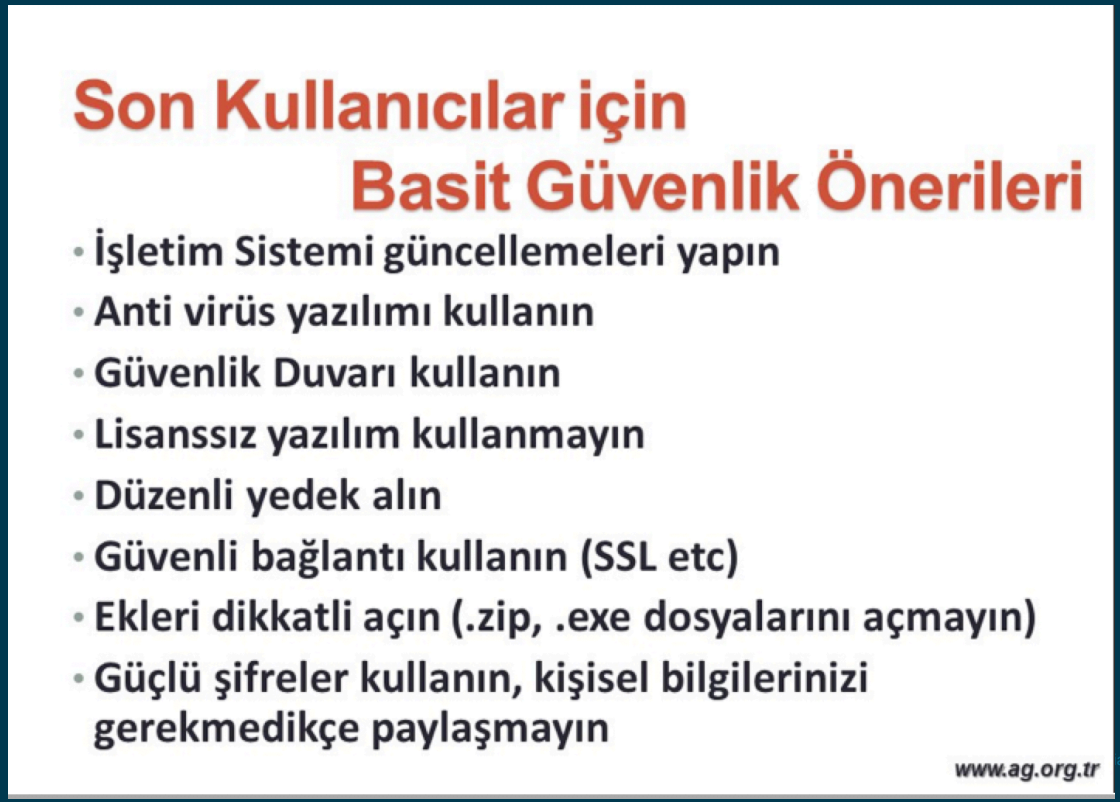
a. What kind of information do you share with social media sites?

1) Everything; I rely on social media to keep in touch with friends and family. (3 points)
2) Articles and news I find or read (2 points)
3) It depends; I filter out what I share and with whom I share. (1 point)
4) Nothing; I do not use social media. (0 points)

3.3 Bölüm Özeti

Güvenlik bir ürün değil, bir SÜREÇTİR!

Bruce Schneier



Özet

- Cihazlarınızı ve ağınızı tehditlerden nasıl koruyacağınızı açıklayın.
- Veri bakımı için güvenli prosedürleri açıklayın.
- Güçlü kimlik doğrulama yöntemleri kullanarak ve güvenli çevrimiçi davranışlar uygulayarak gizliliğinizi nasıl koruyacağınızı açıklayın.

TEŞEKKÜRLER
Arzu KİLİTCİ CALAYIR
https://medium.com/@arzukilitcicalayir

Kaynak : Cisco Ağ Akademisi
(https://www.netacad.com/portal/teaching)
Kaynak - Çeviri: Ağ Yöneticileri Derneği
(http://www.agyoneticileri.org/)

08.04.2020