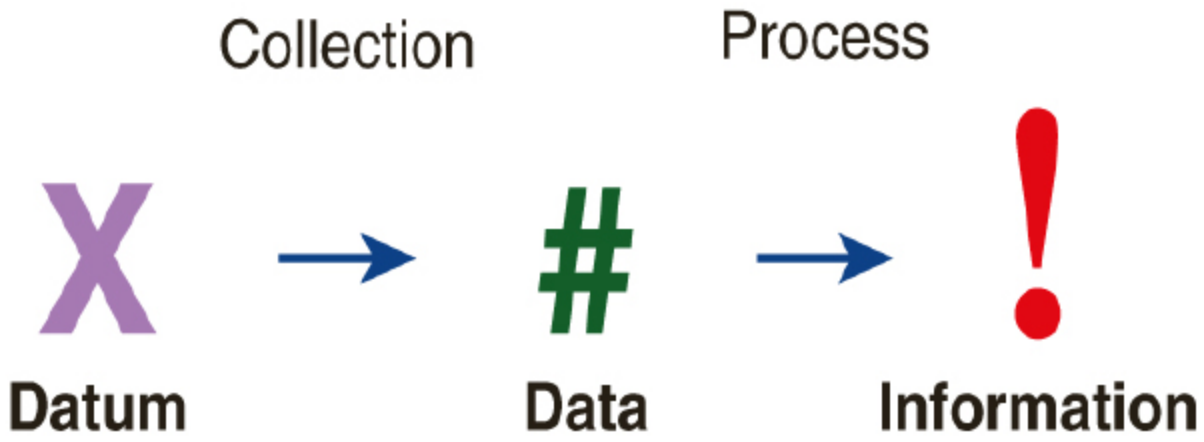
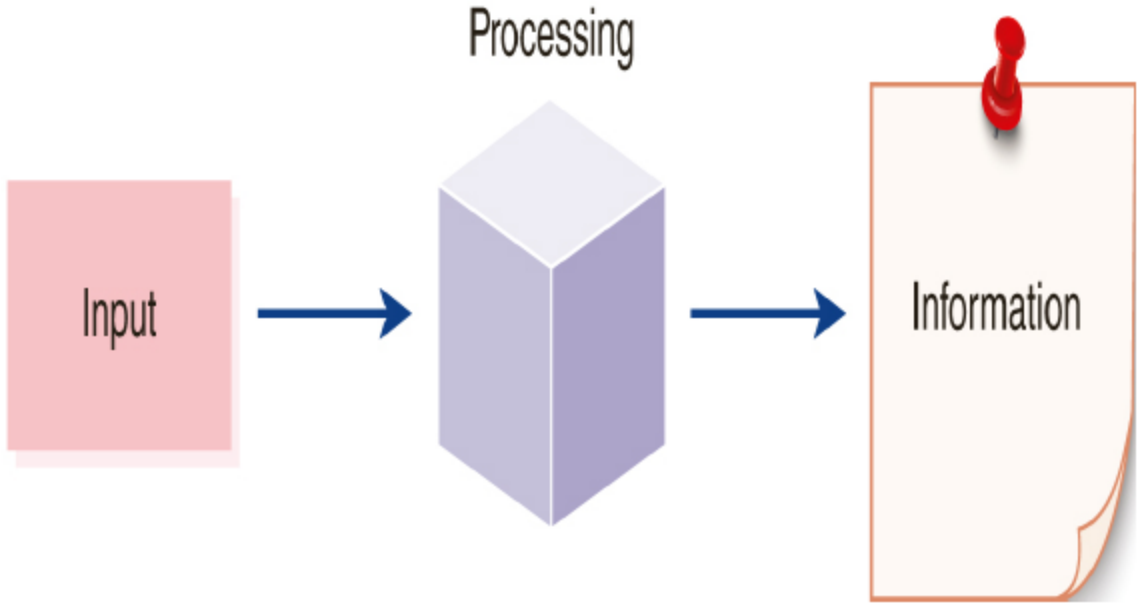
VI. Počátky a bezpečnost na webu

Úvod

- bezpečností je myšleno způsob nakládání s poskytovanými a získanými daty
- data vs informace



- informace = zpracovaná data
  - IPO model (Input, Processing, Output)



- data je třeba chránit

- počátky internetu
  - cílem bylo nahradit telegrafní komunikaci, kterou bylo možné odposlouchávat a lehce zničit
  - vytvořila se první počítačová síť
- 1969 ARPANET
  - napřímo spojené PC
  - propojení univerzit

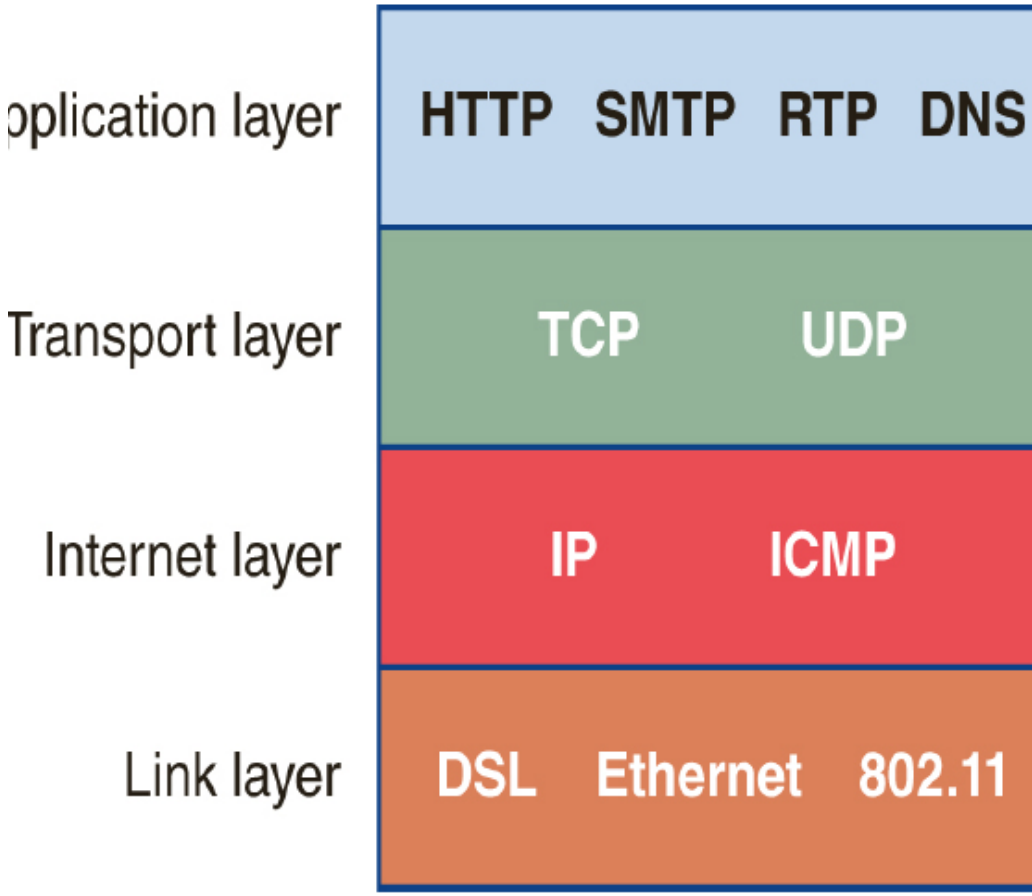
TABLE 1-2 The Growth of the ARPAnet

Date	Total Nodes
October 1969	2
December 1969	4
June 1970	9
December 1970	13
September 1971	18
August 1972	29
September 1973	40
June 1974	46
July 1975	57
June 1981	213

- 1970 nastaly problémy s počtem uzlů -> TCP - Transmission Control Protocol
  - rozptýlené uzly internetové sítě rozdělil do menších skupin
  - později IP = internet protocol
- pro potřeby ARPANETU bylo vyvynuto:
  - Electronic mail (email) (1971)
  - Telnet (Teletype network) (1972)
  - FTP (File Transfer Protocol) (1973)
  - Domain Naming System (DNS) (1983)
  - Open Systems Interconnection (OSI) Reference Model (1984)
- kvůli nebezpečí ztrátě informace byly vytvořené další separátní sítě (MILNET, ...)

TCP/IP

- propojení počítačů a sítí do internetu
- čtyři úrovně:
  - aplikační
    - interakce host serveru
  - transportní
    - jak zacházet s příchozím a připravit odchozí
  - inernetová, síťová
    - adresování, předávání a směrování
  - síťové rozhraní
    - vhodné "packaging" před umístěním zprávy na fyzické médium sítě



- TCP/IP zahrnuje několik dílčích protokolů
  - TCP
    - na transportní úrovni
    - výtvor a ovládání přenosu
  - IP
    - udává strukturu, interpretaci a přidělování internetové adresy
  - HTTP (Hypertext Transfer Protoco)
    - transport obsahu webu
    - HTTPs = zabezpečená verze
  - Emailové protokoly
    - Post Office Protocol (POP3) a Simple Mail Transport Protocol (SMTP)
  - FTP (File Transfer Protocol)
    - transport souboru

Počátky internetu

- přímé připojení k serveru, rychlost 300 bps až 2400 bps
- přesun k jiné službě znamenalo zavěsit
- od 1991 World Wide Web
  - rozvoj HTML (Hypertext Markup Language)
  - UDI (Universal Document Identifier)
    - Universal (or Uniform) Resource Locator (URL)
  - libWWW = první volně dostupný prohlížeč
    - 1995 — Microsoft Internet Explorer, 1999 - Mozila, 2004 - Safari, 2008 - Chrome

Fáze vývoje WWW

PHASE	SPAN	CHARACTERIZATION	FOCUS
Web 1.0	1994–2000	• The Information Web • Static/Read-Only Web	• Static pages for the user's visit • The use of frames or framesets • HTML forms sent via email
Web 2.0	2000–2010	• The Social Web • Read-Write Web	• Sharing content • Blogs and wikis • Web applications
Web 3.0	2010–2020	• The Semantic Web • The Personalized Web	• On-demand dynamic content • Active user involvement • Mobile device access
Web 4.0	2020–	• Intelligent Web	• Focus on individuals • Internet as world computer

Bezpečnost

Aneb jak zabezpečit data a PC

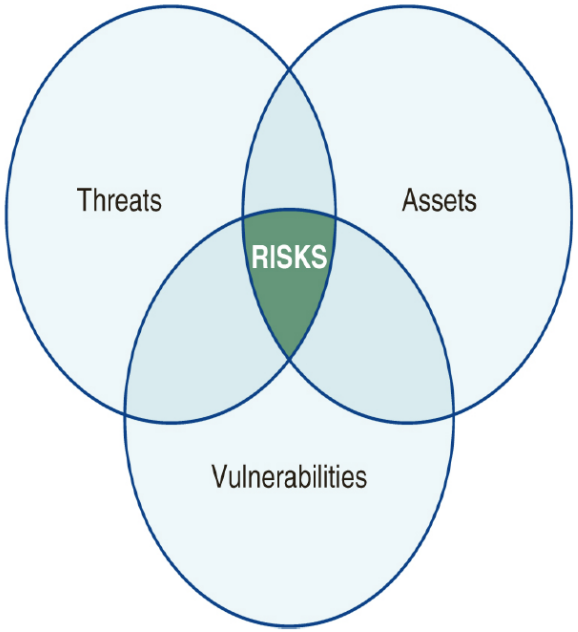
Bezpečnost

- schopnost uchovat hodnotu majetku
- schopnost neztratit cas (potrebny pro napravu)
- SOHO - bezpečnost týkající se domova a malých firem

Zranitelnost, Hrozba, Riziko

- pojmy utvářející potřebu pro zabezpečení

1. **Zranitelnost**
    - "dveře" do domácnosti
    - web může být zranitelný díky svým slabostem, útočník může přistoupit nejen k HTML kódu...
2. **Hrozba**
    - objevená zranitelnost, způsob využití zranitelnosti
    - malware, ransomware
3. **Riziko**
    - ztráta způsobená hrozbou
    - pravděpodobnost hrozby



- zranitelnost je často softwarového původu
- lze ji minimalizovat pravidelným updatem softwaru, aktualizací hesel, ...
- zranitelnost odhaluje počítač, síť nebo webovou stránku a jejich zabezpečení v jedné nebo více z následujících oblastí:
  - **důvěrnost**
    - citlivá data a informace je třeba střežit
  - **integrita**
    - konzistence, přesnost a spolehlivost údajů by měly být udržovány po celou dobu jejich životního cyklu
    - ochrana dat při přenosu, přístupu i během uložení
  - **přístupnost**
    - hardware, software a datové zdroje by měly být trvale přístupné oprávněným uživatelům

Lidská zranitelnost a chyby

- běžné chyby uživatelů
  - neodhlášení se, nezamknutí či nevypnutí systému
  - poskytnutí osobních údajů neověřeným stranám ("phishing")
  - nechání koukat nám přes rameno
  - vyhození citlivých údajů do volně přístupného koše
  - třeba vyvarovat se PEBKAC
    - *"Problem Exists Between the Keyboard And the Chair"*

Heslo

- síla hesla je častý problém běžných uživatelů
- nejběžnější heslo je *password* a případné kombinace
- síla hesla je udávána jeho délkou a různorodostí použitých symbolů
  - ideálně až 16 znaků, držet se nahodilosti
- silné heslo je třeba chránit
  - nepoužívat stejné heslo pro různé účely
  - nepoužívat pro heslo osobní údaje
  - uchovávat heslo zabezbečeně (lístek schovat do trezoru)
  - používat manager na hesla

Nebezpečné umístění

- proti hrozbám je třeba se schránit nejenom softwarově ale i fyzicky
  - kontrola přístupu k zařízení,

Zálohovat, zálohovat, zálohovat

- čím častěji, tím lépe

Přírodní nebezpečí

- záplavy, tornáda, ...

Hrozba

- "aktéři hrozby" (útočníci, hackeři) lze rozdělit na:
  - kyberteroristi
    - jedinný cíl...způsobit škodu a zkázu
  - státem placení zločinci
  - kyberzločinci
    - chtějí ukrást osobní data či peníze pro osobní potřebu
  - Hacktivismus
    - Wikileaks
  - a další

Malware a Ransomware

- *malicious software* (zlomyslný program)
- *ransom software* (vyděračský program)
- software na zaheslování, ukradení, poškození či zničení dat

Malware

- zaměřuje se převážně na:
  - kopírování a zničení citlivých informací
  - *sběr* kreditních karet a dalších finančních dat
  - nakažení počítače pro sběr hodnotných dat nebo na těžbu kryptoměn
  - převzetí kontroly nad více počítači pro útok na server
  - klamání pro krádež osobních dat od cílové oběti
- často při útoku je použito více typů pro odhalení různých zranitelností

Počítačový virus

- malware se specifickou funkcí
- umí se *kopírovat a rozšiřovat*
- roztřídění do skupin:
  - poškozovači souborů
    - proniká do spustitelných souborů a infikuje samostatný počítač
  - makro viry
    - typicky v zip souborech, využívá soubory používající makra
  - polymorfní viry
    - dokáží se přizpůsobit změnou svého kódu

Typy počítačových virů

- Keylogger
  - snímá stisky jednotlivých kláves
- Rootkit
  - usnadňuje nahrávání škodlivých programů do počítače
- Trojský kůň
  - umožňuje útočníkovi přístup do systému
- Spyware
  - zachycuje a ukládá webové aktivity
- Červ
  - software, který se replikuje do cílových souborů operačního systému a běží, dokud nevyprázdní obsah diskové jednotky

Riziko

- vyjádřeno dvěma měřítky
  - pravděpodobnost, že se vyskytne hrozba
  - cena škod po hrozbě
- typy:
  - *Third-party risk* (hrozba třetích stran)
    - přístup dalších stran k interním systémům může představovat riziko
  - *Insider risk* (vnitřní hrozba)
    - vnitřní zaměstnanci jsou potenciální riziko, mohou získat neoprávněně přístup k datům
  - *Compliance risk* (nedodržení standartů)
    - nedodržení předpisů, norem nebo směrnic týkajících se ochrany osobních údajů a majetku

Hodnocení hrozby

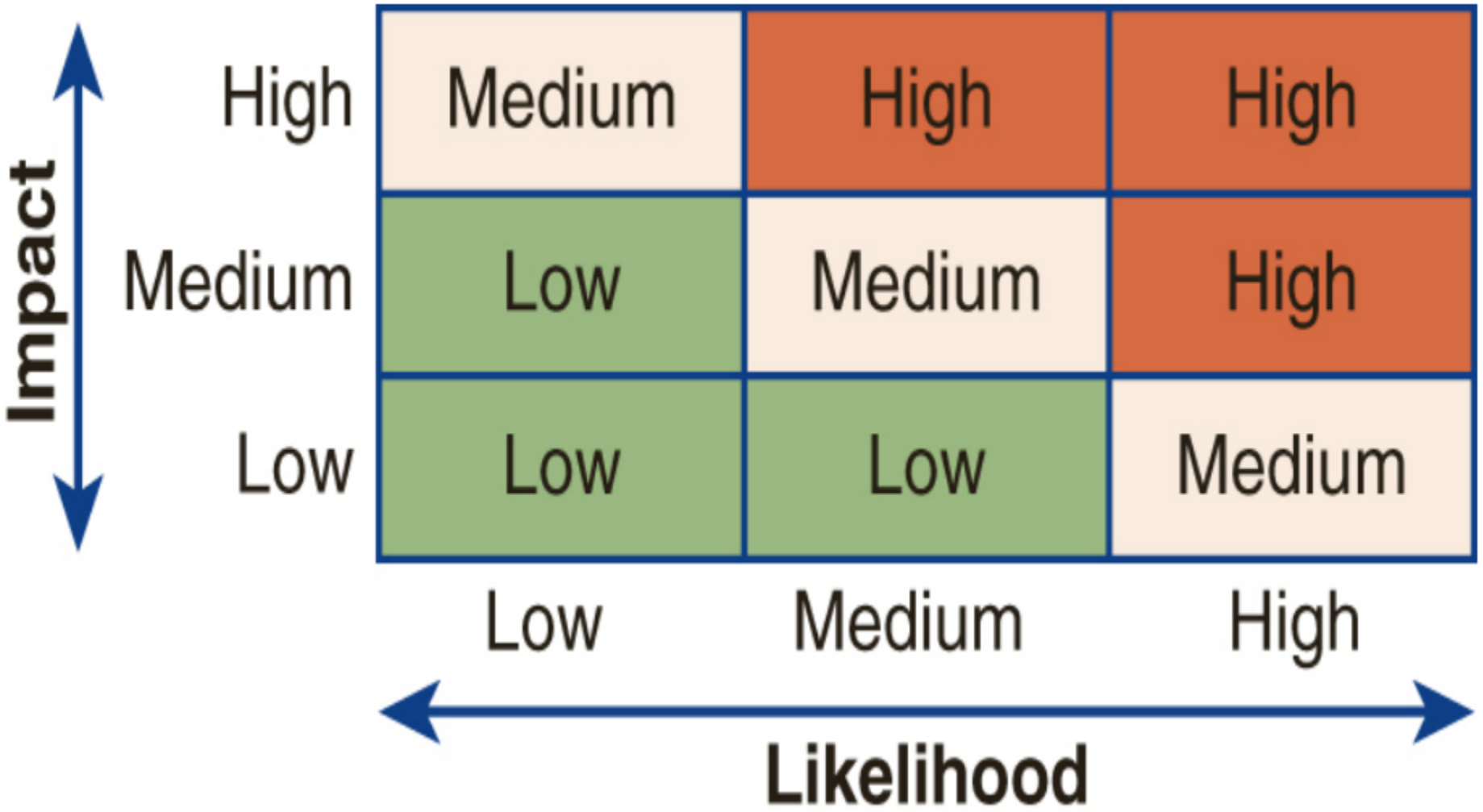
- zahrnuje čtyři kroky
  i. **Identifikace**
    - zjištění potenciálních hrozeb pro systém, web

  ii. **Definice**
    - určení kritérií pro hodnocení závažnosti rizik

  iii. **Analýza**
    - na základě předchozích kroků analyzování daných rizik

  iv. **Prioritizace**
    - určení hodnocení na základě pravděpodobnosti a závažnosti rizik

Matice hrozeb



Ochrana osobních dat

- osobní data jsou často hlavním cílem malwaru
- častý problém při nakládájí s citlivými údaji na sociálních sítích

zásady bezpečnosti

1. Použijte vhodná bezpečnostní nastavení svého prohlížeče, která doplňují nastavení poskytovatele internetových služeb (ISP).
2. Poskytněte pouze požadované informace. Pokud informace nejsou vyžadovány, neposkytujte je. Ještě lépe je, pokud se vám zdá, že množství požadovaných informací přesahuje rozsah účel jejich poskytnutí, možná budete chtít zvážit jiný způsob jejich poskytnutí dokončení daného kroku, pokud vůbec.

3. Na stránkách sociálních médií si prohlédněte zásady a nastavení zabezpečení, včetně těch, které určují, kdo může vidět vaše příspěvky, obrázky nebo aktualizace. Ačkoli je zabezpečení většiny sociálních sítí složité, na webu najdete stránky, které vás provedou procesem vhodného nastavení zabezpečení vašeho účtu.
4. Ujistěte se, že skutečně znáte lidi, od kterých přijímáte pozvánky nebo které si přidáváte na sociální sítě. Ne každý, kdo se chce stát vaším přítelem, kontaktem nebo spojením, je vždy tím, za koho se vydává.
5. Nezapomeňte, že stránky sociálních médií si mohou prohlížet i lidé mimo skupinu vašich přátel, včetně potenciálních zaměstnavatelů, vysokých škol a dalších lidí, na které chcete zapůsobit.

Redukování rizik

- projdeme základní chyby a potenciální rizika

Předpoklady pro hrozby

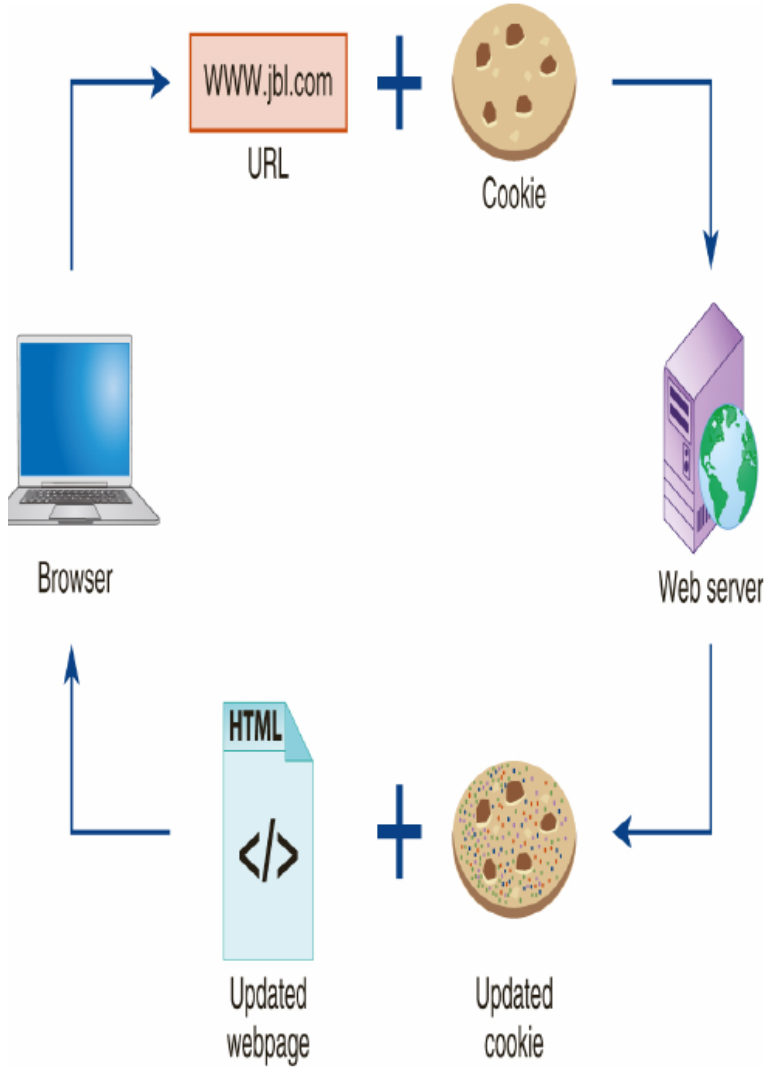
- původní či nezměněná hesla
- nepoužité aktualizace softwaru a firmwaru
- konfigurační chyby
  - defaultní konfigurace není vhodná na vše
- nezašifrovaná externí média
- slabá či neexistujíc kontrola přístupu

Redukce předpokladů hrozeb

- uživatelská konfigurace
  - silné heslo
  - kontrola nutnosti oprávnění u jednotlivých uživvatelů
- konfigurace sítě
  - zabezpečení serverů
  - pokud se nepoužívá protokol IPv6, vypněte jej; nakonfigurujte název hostitele, doménu, DHCP a přístupové informace pro dva nebo více serverů DNS.
- správa aplikací
  - otestování nainstalovaných aplikací
  - odstranit nepoužívané aplikace
- konfigurace záznamu (logování)
  - zajistit záznam akcí v systému

Cookies

- soubor, který používá web pro personalizaci
- obsahuje údaje jako poslední návštěvu stránek, uživatelské předvolby, ...
- dnes hlavně pro marketingové účely
- umožňují snadnější přístup na dříve navštívené stránky => zranitelnost



- typy cookies
  - trvalé
    - zůstanou na pevném disku, dokud nevyprší jejich platnost, nejsou obnoveny nebo vymazány
  - session
    - uchovávají se dokud stránku nezavřeme, resp. opustíme
    - uchovávají například přihlašovací informace, obsah košíku

Bezpečnostní dopady typů cookies

- **HTTP-only cookies**
  - nelze přečíst interprety na straně klienta, jako je například JavaScript, což znamená, že je odolný proti zachycení při útoku XSS (využívá bezpečnostních chyb ve skriptech). Jsou však náchylné k útokům typu XST (zneužívající metodu HTTP TRACE) a CSRF (nezamýšlený požadavek pro vykonání určité akce).
- **Same-site cookies**
  - cookies dané domény, obsahuje příznak určující komu lze informace sdělit
- **Secure cookies**
  - pouze pro HTTPs

- **Supercookies**
  - pochází z domén nejvyšší úrovně (TLD), jako jsou .com, .org, .net nebo .info. Mohou také pocházet z kódů zemí TLD, například co.uk, edu.au nebo mil.cn.
  - mnoho prohlížečů je blokuje kvůli potenciálnímu nebezpečí
    -**Third-party cookies**
  - obsahuje informace o aktuálním návštěvníkovi, ale poskytuje je jiná webová stránka, která je pravděpodobně z jiné domény
  - umožňuje více stránkám sledovat daného uživatele
  - plán také přidat na block list

Nastavení Cookies

- pomocí *Set-Cookie* v http záhlaví odeslaneho z webu
- první request: prohlížeč odešle první požadavek HTTP na domovskou stránku www.example.org

```
GET /index.html HTTP/1.1
Host: www.example.org
...
```

- server odpoví dvěma poli záhlaví Set-Cookie

```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: theme=light
Set-Cookie: sessionToken=abc123; Expires=Wed, 09 Jun 2021 10:18:14 GMT
...
```

- nastavi se 2 typy cookies
  - prvni session cookie (nema expiraci)
  - druhy persistent cookie (udana expirace)

- poté prohlížeč odešle další požadavek na stránku spec.html na webové stránce

```
GET /spec.html HTTP/1.1
Host: www.example.org
Cookie: theme=light; sessionToken=abc123
…
```

- tento požadavek je vztažen k předchozímu
- server odpoví odesláním dané stránky s případnými dalšími *Set-Cookie*
- hodnota cookie může obsahovat libovolný ASCII znak mimo `,` a `;` a mezery `␣`

Struktura cookies

1. Jméno
2. Hodnota
3. Atributy
    - expirace, doména, příznak

Atributy cookies

- atributy slouží prohlížečům k určení, kdy soubor cookie smazat, kdy jej zablokovat nebo zda jej odeslat serveru

Domain and Path

- sdělit prohlížeči, ke které webové stránce soubor cookie patří
- cookies lze nastavit pouze na vrchní doméně aktuálního stránky a jejích subdoménách
- vdefaultně doména a cesta k požadovanému zdroji

- pole hlavičky Set-Cookie v odpovědi HTTP webové stránky po přihlášení uživatele, požadavek HTTP byl odeslán na webovou stránku v rámci subdomény docs.foo.com

```
HTTP/1.0 200 OK
Set-Cookie: LSID=DQAAAK…Eaem_vYg; Path=/accounts; Expires=Wed, 13 Jan 2021 22:23:01 GMT; Secure; HttpOnly
Set-Cookie: HSID=AYQEVn…DKrdst; Domain=.foo.com; Path=/; Expires=Wed, 13 Jan 2021 22:23:01 GMT; HttpOnly
Set-Cookie: SSID=Ap4P…GTEq; Domain=foo.com; Path=/; Expires=Wed, 13 Jan 2021 22:23:01 GMT; Secure; HttpOnly
…
```

- LSID, nemá atribut Domain a atribut Path je nastaven na /accounts. To prohlížeči říká, aby soubor cookie použil pouze při požadavku na stránky obsažené v docs.foo.com/accounts
- HSID a SSID by se použily, když prohlížeč požaduje jakoukoli subdoménu v doméně .foo.com na jakékoli cestě
- předřazená tečka je v nejnovějších normách nepovinná

Expires and Max-Age

- **Expires**: definuje konkrétní datum a čas, kdy má prohlížeč odstranit soubor cookie
- **MAx=Age**: slouží k nastavení vypršení platnosti souboru cookie jako intervalu sekund v budoucnosti

```
HTTP/1.0 200 OK
Set-Cookie: lu=Rg3vHJZnehYLjVg7qi3bZjzg; Expires=Tue, 15 Jan 2043 21:47:38 GMT; Path=/; Domain=.example.com; HttpOnly
Set-Cookie: made_write_conn=1295214458; Path=/; Domain=.example.com
Set-Cookie: reg_fb_gate=deleted; Expires=Thu, 01 Jan 1970 00:00:01 GMT; Path=/; Domain=.example.com; HttpOnly
```

- lu, vyprší někdy 15. ledna 2043
- made_write_conn, nemá datum vypršení platnosti
- reg_fb_gate, má hodnotu změněnou na deleted s dobou platnosti v minulost

Secure and HttpOnly

- nemají přiřazenou hodnotu
- **Secure**
  - omezit komunikaci se soubory cookie na šifrovaný přenos a nařídit prohlížečům, aby soubory cookie používaly pouze prostřednictvím zabezpečených/šifrovaných spojení
- **HttpOnly**
  - nařizuje prohlížečům, aby nezveřejňovaly soubory cookie jinými kanály než prostřednictvím požadavků HTTP (a HTTPS)
  - nelze přistupovat prostřednictvím skriptovacích jazyků na straně klienta, odolné vůči cross-site scripting

Nastavení prohlížeče

- úplně povolit nebo zakázat soubory cookie tak, aby byly vždy přijímány nebo blokovány
- zobrazení a selektivní odstranění souborů cookie pomocí správce souborů cookie
- úplně vymazat všechna soukromá data včetně souborů cookie

Sušenkový zákon

- webový server musí poskytnout uživateli informaci o používání cookies a získat jeho souhlas ještě před tím, než se cookie uloží do uživatelova počítače

Alternativy cookies

- **Flash cookie**
  - spravovány plug-inem Adobe Flash a jsou mimo kontrolu prohlížeče
  - využívány k obnově hodnot HTTP cookies v případě, že uživatel HTTP cookie smazal
- **HTML 5 DOM storage**
- **Microsoft Silverlight cookies**
  - data uložená v plug-inu Silverlight
- **Microsoft Internet Explorer User Data Persistence**
- **Google Gears data**

Zranitelnost bezdrátových sítí

- data mají tři stavy: data v klidu, data v používání a data v provozu
- přenášená data jsou zranitelná převážně při bezdrátovém přenosu
- pokud bezdrátové síťové služby jsou volně dostupné bez nějaké formy ověření nebo autorizace, bezdrátový signál je ve *vzduchu* a je přístupný komukoli v dosahu a ze své podstaty není bezpečný

- typy útoků
  - **fyzické vniknutí**
    - všechna přenosná elektronická zařízení, chytré telefony, notebooky, tablety a další zařízení se mohou připojit k bezdrátovému RF signálu
  - **zlé dvojče**
    - vložení do sítě přístupový bod nebo směrovač
    - útočník je pak schopen zachytit síťový provoz, včetně provozu na internetu a webu

- typy útoků II
  - **válečná jízda (War driving)**
    - válečný řidič je osoba, která se pohybuje v sousedství, ve městech a na jiných místech, kde je přítomna jedna nebo více soukromých bezdrátových sítí
    - útočník se může připojit k síti, nainstalovat malware nebo si jen poznamenat umístění bezdrátové sítě a pokračovat dál
    - vaše bezdrátová síť může být nyní v místní bezdrátové síti otevřená pro hackerskou mapu

- typy útoků III
  - **neoprávněné sdílení souborů**
    - zabezpečené veřejné bezdrátové sítě mohou být bezpečnostní problém z mnoha důvodů
    - jeden z nich se vyskytuje u bezdrátových přenosných počítačů s nezabezpečeným sdílením souborů
    - hackeři mohou mít přístup ke všem adresářům a souborům, které jsou nakonfigurovány pro sdílen

Minimalizace rizik s bezdrátovou sítí

- silná hesla, omezený přístup, data anti-malware software, hlídané souborů sdílení

Media Access Control (MAC) Address Filtering

- připojí se pouze zařízení s danou MAC adresou
- lze bohužel překonat tak, že narušitel podvrhne adresu MAC, která je na schváleném seznamu, pokud zná identifikátor sady služeb (SSID)

Šifrování dat při přenosu

- šifrování dat přenášených prostřednictvím bezdrátové sítě zabraňuje narušiteli který tato data zachytí, aby si je prohlédl
- šifrovací protokoly
  - Wired Equivalency Protection (WEP)
    - staré, není dobrý
  - Wi-Fi Protected Access (WPA)
  - WPA, version 2 (WPA2)
  - WPA, version 3 (WPA3)

Střežení identifikátoru SSID

- SSID (Service set identifier) = identifikační kód přidělený uživatelem pro přístupový bod bezdrátové sítě
- přístupové body, routery a další kontrolní zařízení mají výchozí SSID přiřazený výrobcem (TP-Link_123456)
- SSID by měl být změněn ihned po instalaci přístupového bodu nebo jiného zařízení

Identifikace hrozeb a rizik

- otázka: Proti čemu se máme bránit?
- proti všemu -> nákladné a téměř nemožné

Mapa hrozeb

- https://cybermap.kaspersky.com/, https://threatmap.bitdefender.com/

Identifikace aktuálních hrozeb

- OWASP Top 10 je standardní dokument pro informovanost vývojářů a zabezpečení webových aplikací. Představuje širokou shodu ohledně nejkritičtějších bezpečnostních rizik pro webové aplikace.
  - https://owasp.org/www-project-top-ten/

Bezpečný web a webové aplikace

- původně obsahoval web pouze informace
  - absence uživatelské interakce
- dnes uživatel interaguje s webem různými způsoby
  - nesprávně ověřený a nedůvěryhodný vstup uživatele představuje bezpečnostní riziko
  - zavedeny metody pro ověření vstupu … klíčová obrana

Zásady ochrany:

- Nespoléhejte se pouze na ověřování na straně uživatele
  - prostřednictvím prohlížeče, lze záměrně obejít (vypnutím JavaScriptu v prohlížeči)
- Zajistěte ověření na straně serveru
  - řetězce, znaky a jakákoliv jiná syntax, která může být potenciálně nebezpečná
  - nelze tak snadno obejít
- Použijte *bílou* a *černou* listinu
  - všechna data na blacklistu jsou zamítnuta
  - blacklist je třeba updatovat
  - whitelist obsahuje správnou syntaxi vstupu, vše co není na whitelistu je zamítnuto = odolnější vůči útokům, těžké vytvořit

Zásady ochrany:

- Předpokládejte, že jakýkoliv vstup je *zlomyslný*
  - kontrola jakéhokoliv vstupu jako potenciálně nebezpečného
- Ošetřete svůj vstup
  - vstup je ošetřen, zkontrolován, zda neobsahuje potenciálně škodlivý kód a upraven podle předem stanovených, přijatelných pravidel

Bezpečnostní rizika HTML

```
<form>
First name:
<input type="text" name="firstname" />

Last name:
<input type="text" name="lastname" />
</form>
```

- útočník může skrze nezabezpečený formulář modifikovat web
- zlomyslné tagy lze vložit do nezabezpečených online for
  - `<script>, <embed>, <object>,  <applet>`
- je třeba pečlivě monitorovat vstup, kontrolovat kód stránek, zda nebyl pozměněn (třeba jen kontrolou velikosti souboru)

Common Gateway Interface Script (CGI)

- standard, který definuje metodu, pomocí níž může webový server získávat data z databází, dokumentů a jiných programů nebo je do nich odesílat a prezentovat je uživatelům prostřednictvím webu
- napsáno v jazyce Perl, C++, ASP
- spuštěno serverem po nějaké vstupní akci (předání dotazníku na server, nákupního košíku, ...)
- při výtvoru třeba dbát na bezpečnost, aktualizovat program podle aktuálních zranitelností a hrozeb

Bezpečnostní rizika JavaScript

- interaktivní elementy, které lze vkládat přímo do HTML

```
<script type="text/javascript"> document.write ("Text goes here."); </scritp>
```

- při načtení stránky může být na vašem zařízení spuštěn spuštěn libovolný kód
- JavaScript přímo zamezuje vytváření, zápisu a mazání souborů na straně uživatele

SQL Database Back-End

- back-end databáze je databáze dat, ke které uživatelé přistupují nepřímo prostřednictvím jiné aplikace
- back-endová databáze je předsunuta před webovým serverem, ke kterému pak přistupují klientské prohlížeče
- běžně používané v eshopech na databázi produktů
- lze poškodit jak fyzicky tak třeba *brute-force passsword attack*
- je třeba průběžně zálohovat
- dobré zakomponovat
  - kontrolu přístupu
  - ověřování na základě rolí
  - metody šifrování
  - ověřování integrity

Software development life cycle (SDLC)

- standart definující šest na sebe navazujících fází pří výtvoru webu

1. **Systémová analýza**
    - k čemu software bude složit a co od něj očekáváme
2. **Design**
    - jasné stanovení funcí aplikace
    - jasná podoba vzhledu
3. **Implementace**
4. **Teslování**
    - testování a zkoumání z hlediska chyb, omylů, selhání při vzájemné kompatibilitě, ...
5. **Akceptace a zavedení**
6. **Udržování**

Secure software development life cycle (SSDLC)

- obohacení předchozího postupu o prvky bezpečnosti
- prvek bezbečnosti je přidán v každé fázi SDLC
- standardy SSDLC:
  - NIST SP 800-160 Vol. 1 (U.S. federal agencies)
  - Microsoft Security Development Lifecycle (Microsoft SDL)
    - https://www.microsoft.com/en-us/securityengineering/sdl
  - OWASP Application Security Verification Standard (ASVS), Software Assurance Maturity Model (SAMM)

Strategie bezpečnosti webu a webových aplikací

- nelze použít jen jednu metodu zabezpečení, je třeba použít více vrstev bezpečnosti
- **zabezpečení perimetru**
  - ochrana vnitřní sítě před útoky z okolí
  - antivirus/anti-spyware/antispam/anti-phishing software, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and firewalls
- **host-based zabezpečení**
  - host-based firewalls, IDS antivirus, XSS filtry prohlížeče
- **vzdělávání koncového uživatele**
  - informace o nejnovějších webových útocích, jejich účelu a o tom, jak jim mohou koncoví uživatelé předcházet

- **ověření a správa přístupu**
- **kontrola vstupu**
- **správa zranitelnosti**
  - aktualizace, pomocí patchů, servisních balíčků a dalších technik k zajištění aktuálního zabezpečení webových stránek a aplikací

Zakomponování strategie bezpečnosti do SDLC

Koncept a plánování

- definování bezpečnostních a regulačních cílů projektu
- definice možných hrozeb a strategií pro jejich minimalizaci
- bezpečnostního školení pro všechny členy týmu

Architektura a design

- modelování hrozeb, přezkoumání bezpečného návrhu, a identifikaci případných zranitelností v externím softwaru

Implementace

- přezkoumání a prosazování postupů bezpečného programování a používání nástrojů statického skenování aplikací (SAST) https://spectralops.io/
- šifrování, zacházení s chybami

Testování a debugging

- dynamické testování
  - testovat aplikace na zranitelnosti napodobováním hackerských útoků
- fuzz testování
  - do aplikace jsou vkládány náhodně generované vstupy, aby se otestovala schopnost aplikace pracovat s různým obsahem a formáty
- penetration testování (pen test)
  - externí testři simulují útok na aplikaci, resp. web

Uveřejnění a udržování

- připravit se na potenciální hrozby a umět na ně rychle reagovat

Zabezbečené vs nezabezpečené protokoly

- nezabezpečené protokoly pro rychlejší přenos v bezpečném prostředí

Protokol	Jméno	Popis
FTP	File Transfer Protocol	Odesílání a stahování souborů na vzdáleného hostitele a ze vzdáleného hostitele. Umožňuje také základní úlohy správy souborů.
SFTP	Secure File Transfer Protocol	Bezpečné nahrávání a stahování souborů na a ze vzdáleného hostitele. Založeno na Secure Shell (SSH).

Protokol	Jméno	Popis
HTTP	Hypertext Transfer Protocol	Načítání souborů z webového serveru. Data jsou odesílány v otevřeném textu.
HTTPS	Hypertext Transfer Protocol Secure	Načítání souborů z webového serveru. HTTPS používá k šifrování dat mezi klientem a hostitelem protokol SSL/TLS.

Protokol	Jméno	Popis
RCP	Remote Copy Protocol	Kopíruje soubory mezi systémy, ale přenos není zabezpečen.
SCP	Secure Copy Protocol	Umožňuje bezpečné kopírování souborů mezi dvěma systémy. Využívá technologii SSH k poskytování šifrovacích služeb.

Běžné zranitelnosti a hrozby, aneb jak se jim bránit

Hrozba	Ochrana
Škodlivý kód je vložen do query stringu, pole, soubory cookie a hlavičky.	Předpokládejte, že všechny vstupy jsou škodlivé. Omezte, odmítněte a upravte všechny vstupy.
Přenášená data jsou zachycena a zneužita.	Používejte HTTPS protokol.

Hrozba	Ochrana
Citlivé údaje v souborech protokolu a auditních souborech mohou být pro útočníka zranitelné.	Použití zásady nejmenších privilegií a řízení přístupu k omezení přístupu.
Škodlivé používání prolamování hesel, zvyšování oprávnění a sociální inženýrství k ověření totožnosti.	Vzdělávejte uživatele v oblasti zabezpečení hesel, šifrujte hesla a prosazujte důkladné zásady používání hesel.

Hrozba	Ochrana
Škodliví uživatelé získají přístup k omezeným a citlivým datům nebo prostředkům.	Šifrování datových souborů a adresářů. Validujte a ověřte způsob autorizace.
Škodliví uživatelé, kteří jsou schopni zmocnit se relace a použít platné přihlašovací údaje.	Ruční odhlášení z relací. Automatické odhlášení uživatelů z relací po určité době nečinnosti.
Skrytí nebo ignorování souboru, složky nebo umístění zdrojů.	Zabezpečení prostřednictvím skrytého přístupu obvykle nestačí. Používejte mechanismy řízení přístupu a zabezpečení oprávnění.