INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Université Polytechnique HAUTS-DE-FRANCE

Sécurité des Services

II. Mesures générales qui s'appliquent à toutes les attaques

Assurer une sécurité robuste contre les cyberattaques nécessite une approche multi-facettes, par uniquement technique, qui couvre tous les aspects d'un système qui, ensemble, forment peuvent résister à diverses formes d'attaques peu complexes et protéger à la fois les systèmes et les données.

1. **Durcissement du système** : Il s'agit de réduire les vulnérabilités en désactivant les services inutiles, en limitant les privilèges d'accès et en configurant correctement les logiciels.
2. **Mise à jour et gestion des correctifs** : Gardez vos systèmes à jour avec les derniers correctifs de sécurité et assurez-vous que toutes les mises à jour sont correctement installées.
3. **Sécurisation des protocoles applicatifs** : Utilisez des protocoles sécurisés comme HTTPS et TLS pour protéger les données en transit.
4. **Authentification robuste** : Implémentez une politique de mots de passe forte et considérez l'utilisation de l'authentification multi-facteurs.
5. **Contrôles d'accès** : Utilisez le principe du moindre privilège, qui stipule que les utilisateurs ne doivent avoir que les privilèges d'accès nécessaires à l'exécution de leurs tâches.
6. **Formation et sensibilisation à la sécurité** : Formez les utilisateurs aux bonnes pratiques de sécurité et à la reconnaissance des signes d'une cyberattaque potentielle.

1.4. Importance de la sécurité des réseaux

1.4. Importance de la sécurité des réseaux

a) Protection des données sensibles :

- **Financières**
- **des données médicales,**
- **secrets industriels.**

1.4. Importance de la sécurité des réseaux

a) Préservation de la réputation et de la confiance :

avoir un impact négatif

réputation

1.4. Importance de la sécurité des réseaux

Conformité aux réglementations :

Règlement général sur la protection des données (RGPD)

loi américaine sur la protection des données de santé (HIPAA).

1.4. Importance de la sécurité des réseaux

d) Prévention des attaques et des intrusions :

constamment menacés par des attaques

1.4. Importance de la sécurité des réseaux

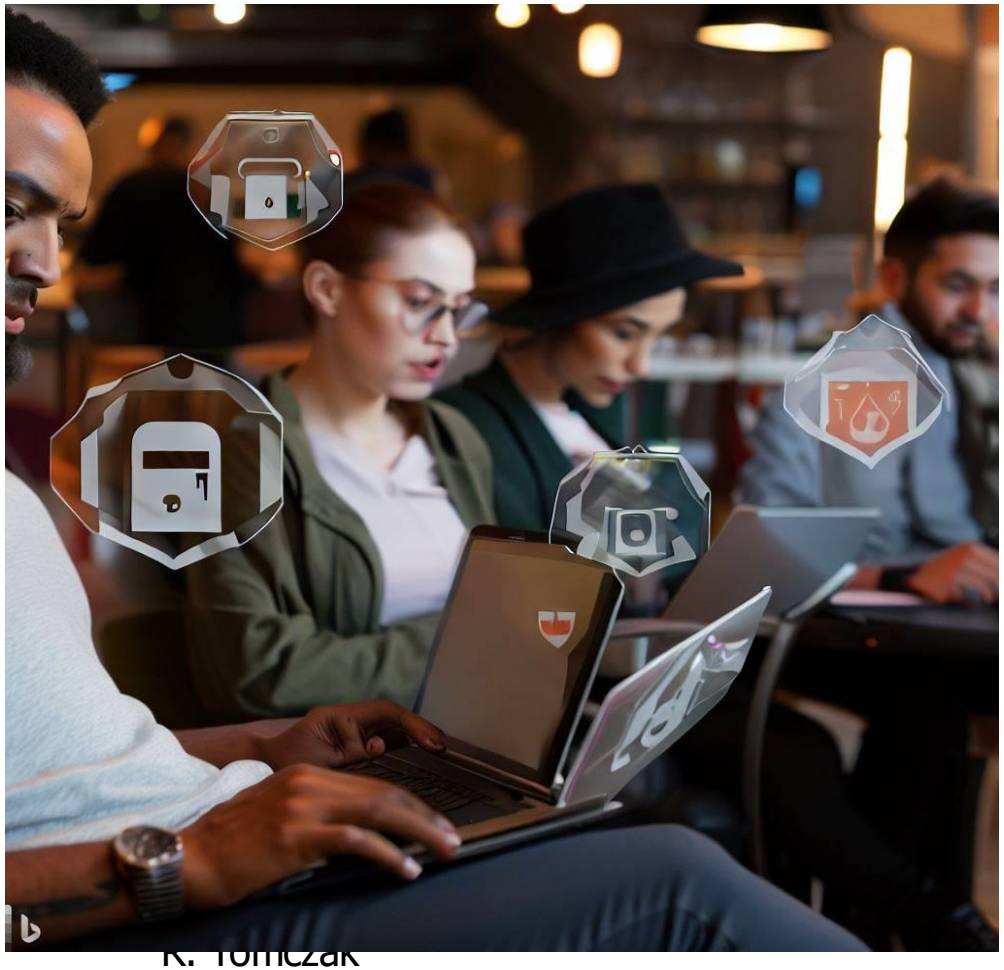
e) Continuité des activités et résilience :

assurer la continuité des activités

1.4. Importance de la sécurité des réseaux

f) Sécurité des utilisateurs et de leurs appareils :

les logiciels malveillants, les ransomwares et les attaques de phishing.



X. Attaques visant les services ou également appelée protocoles applicatifs

DHCP

a) DHCP Spoofing

- Le DHCP Spoofing, également appelé DHCP Starvation, est une attaque qui vise à épuiser les adresses IP disponibles dans le pool d'adresses d'un serveur DHCP (Dynamic Host Configuration Protocol).
- L'attaquant envoie un grand nombre de requêtes DHCP avec de fausses adresses MAC, forçant ainsi le serveur à attribuer toutes les adresses IP disponibles.
- Cela peut empêcher les clients légitimes d'obtenir une adresse IP et d'accéder au réseau.

Les attaques par amplification

1. **Protocole DNS (Domain Name System) amplification :**

   - Le protocole DNS est utilisé pour traduire les noms de domaine en adresses IP.
   - Les attaquants exploitent le DNS en envoyant des requêtes DNS avec une adresse IP source falsifiée (l'adresse IP de la victime).
   - Les serveurs DNS répondent avec des informations beaucoup plus volumineuses que les requêtes initiales, créant ainsi une amplification du trafic.
   - Les serveurs DNS ouverts et mal configurés sont particulièrement vulnérables à ce type d'attaques.

- Une attaque notoire de ce type est l'attaque qui a visé GitHub en 2018, qui a atteint un pic de trafic de 1,35 téraoctets par seconde.

Autres exemples

1. **Protocole NTP (Network Time Protocol) :** Le protocole NTP est utilisé pour synchroniser les horloges des systèmes informatiques sur Internet.

➢ Les attaquants exploitent les serveurs NTP en utilisant la commande "monlist", qui renvoie une liste des 600 derniers clients ayant contacté le serveur NTP.

➢ Cette réponse est beaucoup plus volumineuse que la requête initiale, entraînant une amplification du trafic. Les serveurs NTP mal configurés ou non mis à jour sont particulièrement vulnérables à ces attaques.

Protocole applicatif :HTTP.

1. **Attaques par injection de code** : Les attaques par injection de code exploitent les vulnérabilités dans le code d'une application pour injecter et exécuter du code malveillant.

- Par exemple, si une application PHP utilise la fonction `eval()` avec des données provenant directement de l'entrée de l'utilisateur, cela peut permettre à un attaquant d'exécuter du code PHP arbitraire.

```
<?php
$function = $_GET['func'];
eval($function);
?>
```

Si un attaquant envoie une requête comme http://example.com?func=system('ls'), il pourrait lister les fichiers du serveur.

Contre mesure requête préparée

```php
<?php
    $pdo = new PDO('mysql:host=localhost;dbname=mydatabase', 'username', 'password');
    $stmt = $pdo->prepare('SELECT * FROM users WHERE email = ? AND password = ?');
    $stmt->execute([$email, $password]);
    $user = $stmt->fetch();
?>
```

1. **Attaques Cross-Site Scripting (XSS)** : Ces attaques se produisent lorsqu'un attaquant injecte du code malveillant dans une page web, qui est ensuite exécuté par le navigateur de l'utilisateur. Cela peut être utilisé pour voler des informations sensibles, comme les cookies de session, qui peuvent ensuite être utilisés pour usurper l'identité de l'utilisateur.

- Par exemple :
- **http://example.com/search?query=<script>malicious_code_here</script>**

connexions HTTPS sécurisées

- HTTPS utilise
  - le protocole SSL (Secure Sockets Layer)
  - ou TLS (Transport Layer Security)
  - pour fournir une couche supplémentaire de sécurité.

  - SSL et TLS sont des protocoles de cryptographie qui chiffrent les données lorsqu'elles sont envoyées sur un réseau.
    - Cela signifie que même si quelqu'un intercepte les données, il ne pourra pas les comprendre sans la clé de déchiffrement appropriée.

  - Idem telnet avec SSH

XI. Cas particulier des attaques par déni de services (DoS, Botnets et attaques DDOS)

- ***Attaques DDOS (ex. : amplification, réflexion)***

- Il est important de noter que, bien que ces attaques spécifiques ne soient plus généralement efficaces, les attaques DoS et DDoS (Distributed Denial of Service, où l'attaque est menée à partir de multiples systèmes) restent une menace sérieuse. Les attaques DDoS modernes utilisent généralement une grande quantité de trafic pour submerger un système, par exemple en exploitant une botnet pour générer un trafic massif.

- Ces attaques peuvent utiliser la réflexion ou l'amplification vue précédemment

Botnets

- Un botnet est un réseau de machines informatiques infectées par un malware qui permet à un attaquant de les contrôler à distance. Ces "bots" peuvent être utilisés pour une variété d'actions malveillantes, y compris l'envoi de spam, le lancement d'attaques DDoS, la fraude par clics, le minage de crypto-monnaies et bien d'autres.
-
- 1. **Mirai** : est un botnet qui a été utilisé en 2016 pour lancer des attaques DDoS massives, notamment contre le fournisseur de DNS Dyn, ce qui a entraîné des perturbations majeures de nombreux sites web populaires. Mirai se propage en infectant une variété de dispositifs IoT (Internet of Things) avec des sécurités faibles, tels que les caméras de surveillance et les routeurs.

Contre-mesures spécifiques pour les attaques par déni de service

a) Services de mitigation DDoS :

- Ces services utilisent une variété de techniques pour filtrer le trafic lors d'une attaque DDoS, en laissant passer le trafic légitime tout en bloquant le trafic malveillant. Par exemple, comme mentionné précédemment, GitHub utilise le service Prolexic d'Akamai pour se protéger contre les attaques DDoS. Cloudflare est un autre fournisseur populaire de services de mitigation DDoS.

a) Réseau de diffusion de contenu (CDN) :

- Un CDN peut aider à atténuer une attaque DDoS en distribuant le trafic entre un réseau de serveurs. Par exemple, Netflix utilise le CDN de Amazon Web Services pour gérer le trafic élevé et se protéger contre les attaques DDoS.

a) Équilibrage de charge :

- Cela permet de répartir le trafic sur plusieurs serveurs, ce qui peut aider à gérer le trafic supplémentaire lors d'une attaque DDoS. Les grands sites web comme Google et Amazon utilisent l'équilibrage de charge pour gérer le trafic élevé e résister aux attaques DDoS.

Contre-mesures spécifiques pour les attaques par déni de service

a) Limites de taux :

- Cela implique la limitation du nombre de requêtes qu'un utilisateur peut envoyer à un serveur dans un certain laps de temps. C'est une tactique couramment utilisée par les sites web pour prévenir les attaques DDoS.

a) Pare-feu :

b) Un pare-feu peut être configuré pour bloquer le trafic provenant d'adresses IP suspectes ou pour bloquer le trafic si le volume de requêtes dépasse un certain seuil. De nombreux pare-feu modernes ont également des fonctionnalités intégrées pour la détection et la prévention des attaques DDoS.

Contre-mesures spécifiques pour les attaques par déni de service

a) Redondance :

- Avoir des serveurs de secours en place peut aider à maintenir la disponibilité lors d'une attaque DDoS. Par exemple, les fournisseurs de services de cloud tels que Microsoft Azure et Amazon AWS offrent des options pour la redondance et le basculement automatique en cas de panne ou d'attaque DDoS.


INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
HAUTS-DE-FRANCE


Université
Polytechnique
HAUTS-DE-FRANCE