Operating System Security

#08 – Windows Server Hardening

Herman Kabetta

hermanka.github.io

Security Rules

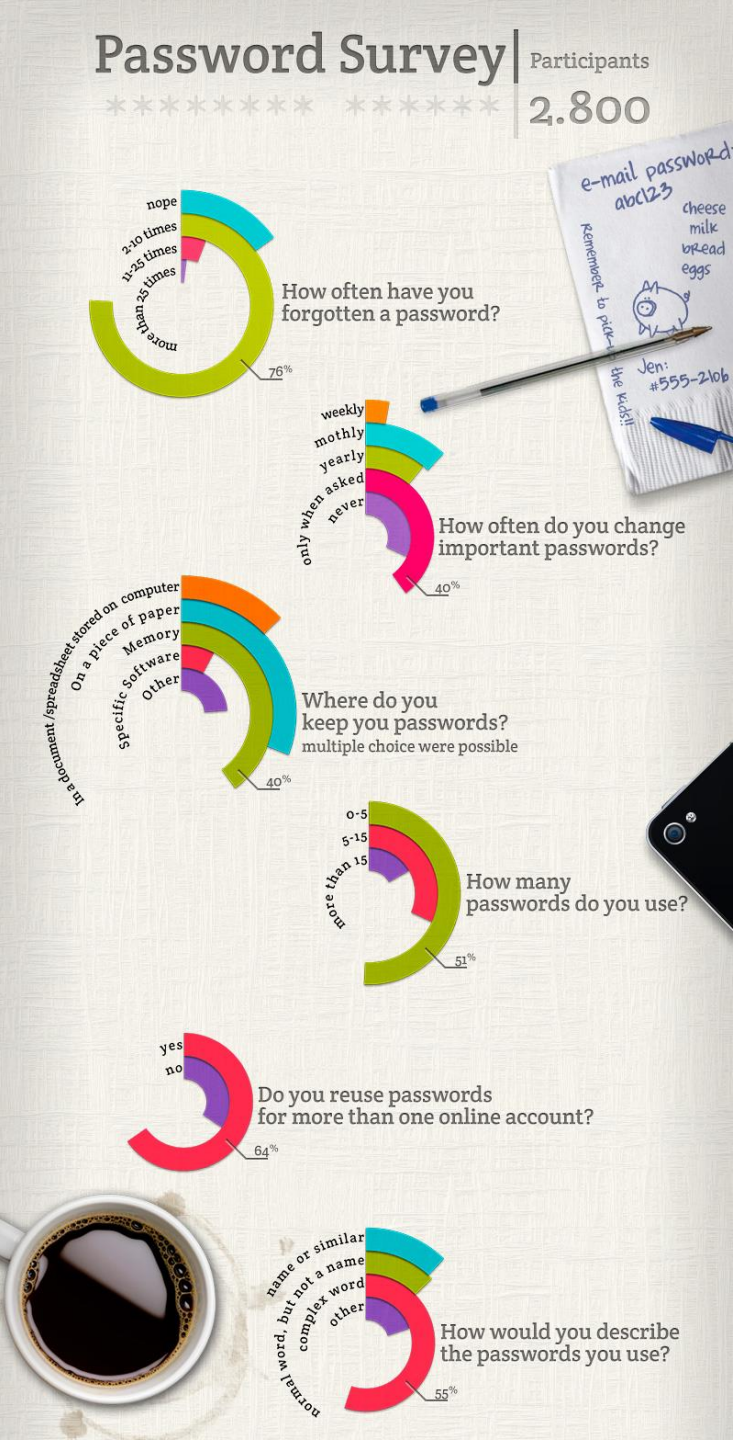
1. Increase Authentication Security
2. Protect Data with Encryption
3. Patch Management is Mandatory
4. Attack Surface Reduction (ASR)
5. Use Mitigation Technologies
6. Install Anti-Virus / Anti-Malware
7. Detection and Notification

1. Increase Authentication Security

- Best practices for user authentication that, if combined with other security measures, will help to increases the overall security of your system
- Threat : Without strong authentication practices, a potential attacker can more easily gain access to your server. The attacker can then utilize your server for malicious activities, take advantage of your server’s resources, or possibly overtake the server, locking you out of it completely.

User Authentication Best Practices

(a) Use strong and complex passwords



User Authentication Best Practices

(b) Never reuse passwords for different services

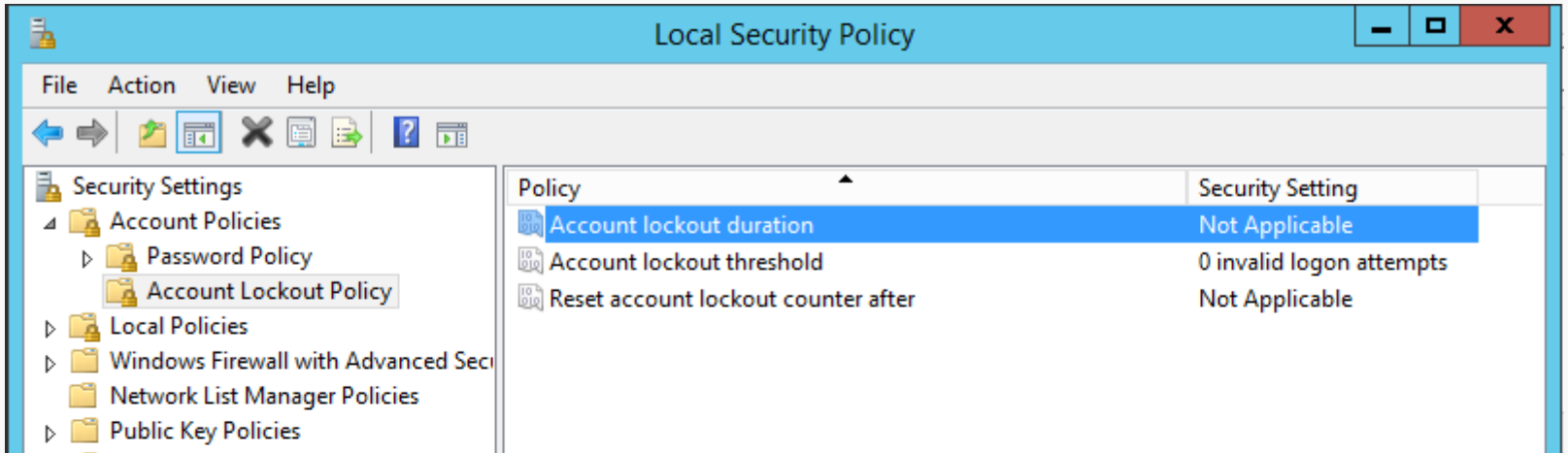
(c) Change the passwords on a regular basis

User Authentication Best Practices

(d) Apply temporary account lockouts to prevent brute force or dictionary attacks

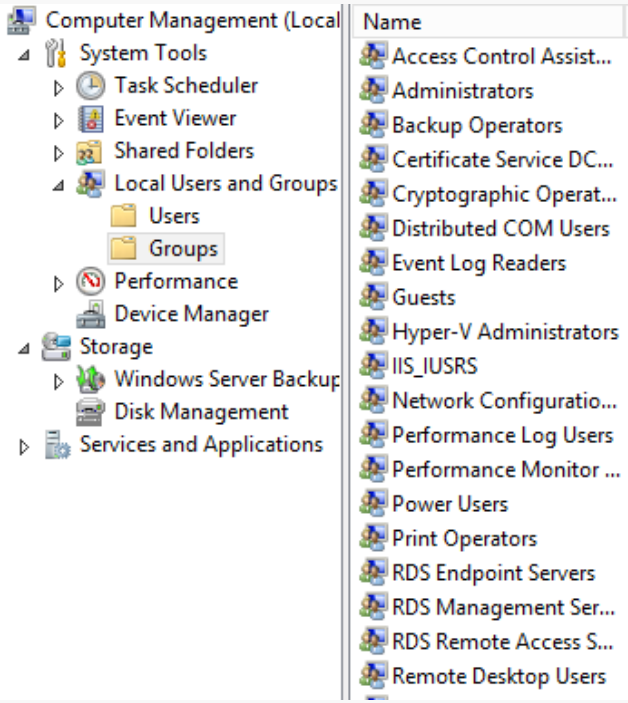
How to configure:

- Click **Control Panel** > **System and Security** > **Administrative Tools**
- Click on the Local Security Policy menu entry
- In the Local Security Policy window select **Account Lockout Policy** (path is: Security Settings/Account Policies/Account Lockout Policy).
- In the details pane, right-click the policy setting that you want.
- Click **Properties**.



User Authentication Best Practices

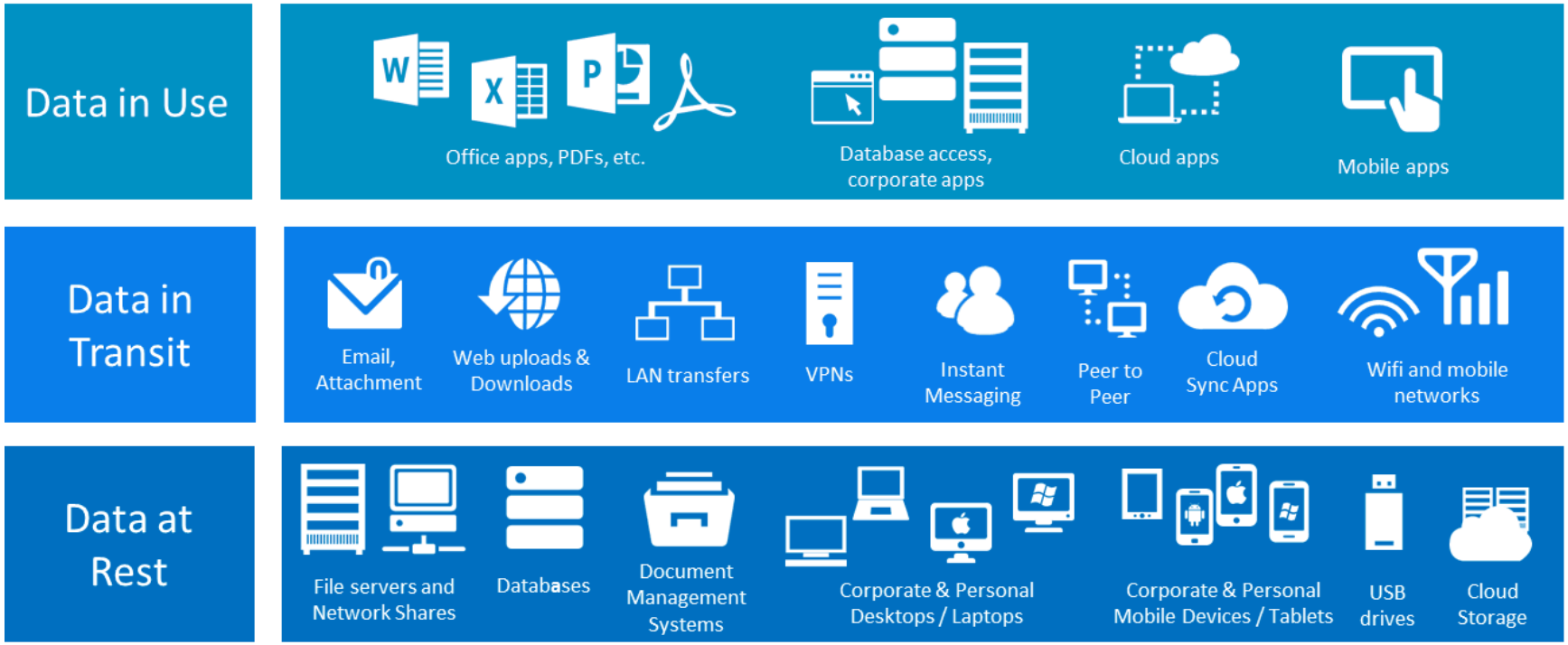
(e) Only allow logins to the system for accounts that need access



In order to verify that, do the following:

- Click the start button.
- In the menu, click **This PC** with the right mouse button.
- Click **Manage**
- In the Server manager, click **Local Server** in the left navigation bar.
- Click **Tools** in the top menu.
- Click **Computer Management**.
- Click **Local Users and Groups**.
- Double-click **Groups**
- Double click the group, you want to edit. For example, **Remote Desktop Users** or **Administrators**.

Make sure that the groups only contain those users who work with the system.



2. Protect Data with Encryption

Threat: Proper usage of encryption can successfully mitigate an attack. Even if your data ends up in the hands of an attacker, he will not be able to access the data without the encryption key

Data State Encryptions

- Data in Transit/Motion
  - Network Level Authentication (NLA) for Remote Desktop
  - HTTPS certificate and enable HTTPS
- Data in Rest
  - BitLocker
  - Encrypted File System (EFS)
  - 3rd party encryption tools
- Data in Use
  - Problem : local attacker with the corresponding privileges can extract fragments of data from memory
  - Advice : Limit access

3. Patch Management is Mandatory

- Threat : If security patches are not applied regularly and in time, attackers can leverage known vulnerabilities present in your software to compromise your system.
- Therefore it is highly recommended to enable automatic updates or manually apply security patches as soon as possible to protect your server from well-known attacks.

4. Attack Surface Reduction (ASR)

The Attack Surface

DEFINITION

The attack surface of an organization is the complete set of attack vectors that an attacker can attempt to exploit to carry out a successful attack. This includes not only **software, operating systems, network services and protocols but also domain names and SSL certificates.**

VISUALIZATION & KEY CONCEPTS

- **Visualization:** mapping out devices, applications, networks, services, etc.
- **Indicators of Exposure (IOEs):** missing security controls, exposed vulnerabilities, unsecure configurations or access rules.
- **Indicators of Compromise (IOCs):** indicator that an attack has already succeeded.

TYPES OF ATTACK VECTORS

The attack vectors might be related to **devices, protocols, interfaces, firmware, operative systems, virtual and cloud networks, ICS & SCADA, applications, services, other physical and digital assets and the human element.**

REDUCING THE ATTACK SURFACE

Organizations can reduce the attack surface by **removing unnecessary software and services, patching all known vulnerabilities, updating all hardware/software and correcting all misconfigurations.** Nevertheless, reducing the attack surface to zero is unrealistic.

DISRUPTING THE ATTACK SURFACE

The end goal is to make life hard for the adversary. The following resilience techniques can help organizations better resist and recover from attacks:

- Adaptive Response
- Deception
- Dynamic Positioning
- Non-Persistance
- Realignment
- Unpredictability

Source: Mitre

4. Attack Surface Reduction (ASR)

Typical and recommended tasks

- Do not run unnecessary applications and services
- Disable Windows Server 2012R2 features that you do not use. For example, if you do not need FTP access, disable it.
- Identify those services and tasks, which are not critical to the management of your network, and then disable the associated system policy rules.
- Limit the applicability of the system policy rules to required network entities only.
- Activate the Window Firewall and allow only inbound and outbound connections that are necessary.
- Use Security Configuration Wizard

5. Use Mitigation Technologies

<u>Threat</u> : An exploit is a piece of code developed to attack a computer system by taking advantage of a vulnerability of that system. In most cases, exploits trigger memory corruption.

- Data Execution Prevention (DEP)
- Address Space Layout Randomization (ASLR)

How to check if the option Turn on DEP for all programs and services is enabled:

- Click **Control Panel** > **System and Security** > **System** > **Advanced System Settings**.
- In the new System properties windows, click the **Advanced** tab.
- In the Performance section, click **Settings**.
- Click the **Data Execution Prevention** tab.

Check if the following setting is selected: *Turn on DEP for all programs and services, except those I select**

- If not, enable this option.

Note: Don´t add exceptions here if you are not aware of the consequences!

6. Install Anti-Virus / Anti-Malware

REGULAR ANTI-VIRUS/MALWARE

ENDPOINT ANTI-VIRUS/MALWARE