Use the Cyber Kill Chain to Secure End-user Devices

Tom Olzak
University of Phoenix

Use the Cyber Kill Chain to Secure End-user Devices

Tom Olzak MBA, CISSP
University of Phoenix

April 2022

End-user devices are the greatest threat to network security, with a generally standard attack path depicted in the Lockheed Martin Cyber Kill Chain, as shown in Figure 1. Use of the kill chain helps identify risks against user devices, both mobile and static, by providing the threat actor's perspective. Breaking links in the chain hinders or prevents a threat actor from compromising a user device and using it as an attack pivot point.

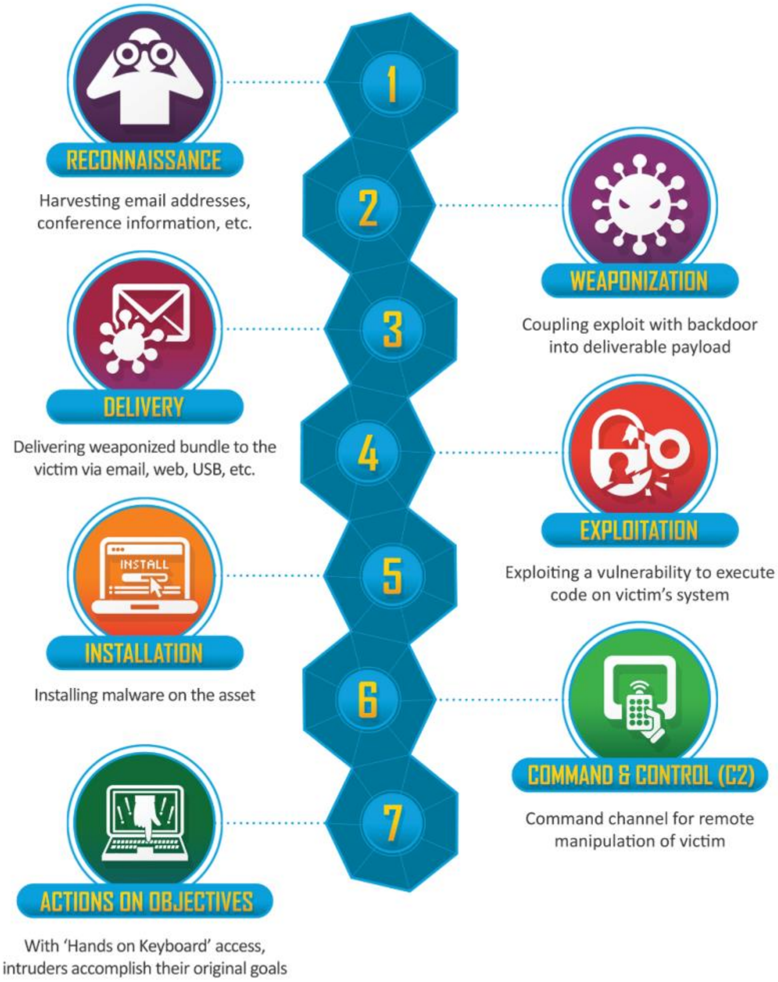
1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Figure 1: Lockheed Martin Cyber Kill Chain (Lockheed Martin, 2022)

Cyber Kill Chain Analysis

Reconnaissance

The first step a threat actor takes in any attack is reconnaissance. Reconnaissance enables the threat actor to learn as much about a target as possible by using publicly available information and network footprinting.

OSINT

Much information is available across public sources. Exploring these resources and collecting relevant information is known as open-source intelligence, or OSINT (Olzak, 2020).

Sources of OSINT on the web include

- Blogs
- Discussion groups
- Any user-created content
- Online publications
- Social networking sites
- Database services
  - Factiva
  - Lexis-Nexis
  - Dialog
- Information stored on internet-facing devices

OSINT resources found off of the web include

- Public government data
- Commercial and professional publications
- Imagery
- Financial and industrial analyses

Most organizations understand that these resources might contain valuable information needed to identify valuable target resources and how to find them. However, other resources, known as gray literature, are less likely to be considered when identifying available OSINT. This is known as gray literature, including,

- Technical reports
- Preprints
- Patents
- Working papers
- Unpublished works
- Newsletters
- Business proposals
- Requests for proposal

Network footprinting

Network footprinting is used by ethical hackers, penetration testers, and threat actors. It gathers information about a network and connected devices, and the resulting data are paired with OSINT to illustrate an organization's attack surface: both human and technology. Figure 2 shows information that can be gleaned from footprinting activities.

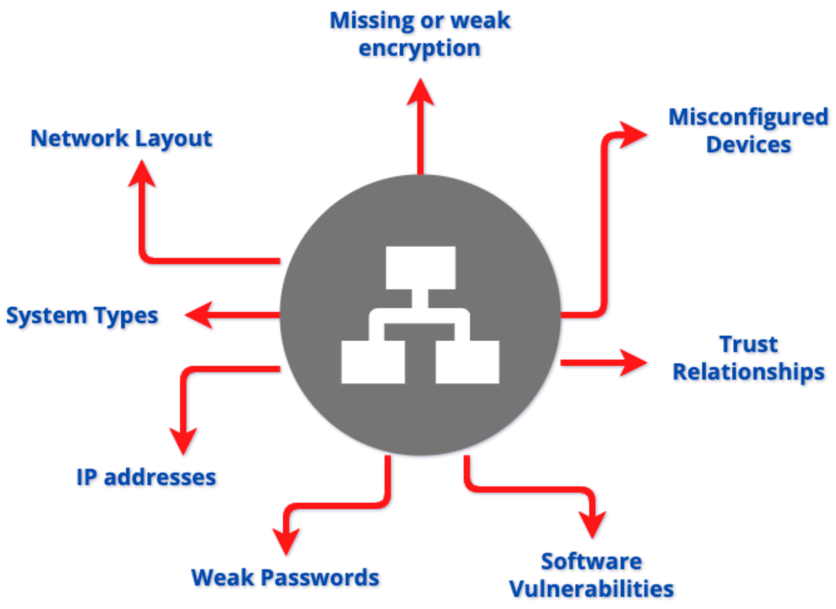

Figure 2: Footprinting Data

Footprinting is done in two ways: active and passive (Zola, 2021). Passive footprinting produces very little that network monitoring can detect. It includes OSINT collection and the use of packet capture and flow analysis software. The capture and analysis software can run on compromised systems or threat actor devices connected to open ports on a target network.

Active footprinting uses tools, techniques, and procedures (TTP) to map networks and identify vulnerabilities. These include running ping sweeps to identify connected endpoints and using traceroute to map network devices. While these TTP are effective, IPS and other monitoring solutions can detect the associated anomalous behavior.

Use of reconnaissance information

Once reconnaissance data is collected, the threat actor can use them to

- Craft social engineering attacks that target specific targets.
- Guess passwords. When a threat actor understands a target user's interests and environments, including family names.
- Understand the organization's network layout and connected devices/systems. This helps determine what should be attacked and why enabling a threat actor to compromise the optimal device to launch attacks against his intended target resources.
- Gain insight into the operating systems and applications running on target resources. This helps a threat actor identify valuable vulnerabilities and known exploits.

A threat actor might not be able to get all the needed information in one place. However, he can gather bits of data across multiple resources that can be aggregated to provide a big picture attack surface.

Reconnaissance defense

It's impossible to sanitize OSINT resources to prevent threat actor access completely. However, an organization can take steps to minimize the effectiveness of reconnaissance.

- Organizations must understand what information is available about them across the web and in public documents. This can help with partial sanitization and adjusted defenses.
- Organizations must control what resources are accessible via the internet. It is not uncommon for employees to place documents on servers or other devices that threat actors can remotely with internet tools.
- Organizations must train employees to help ensure they don't post information potentially usable to threat actors on social media or other publicly accessible places.
- Organizations must control the distribution of project, research, and other sensitive documentation.

An organization can reduce footprinting effectiveness by

- Blocking or disabling all unused network ports
- Using strong authentication, like IEEE 802.1x, to control what can connect
- Segment networks and use segment access control lists to help prevent a connected device from seeing the entire network and all related traffic

Weaponization

The next link in the chain is weaponization. This is when the threat actor uses reconnaissance information to create an attack package with a high probability of success. There is not much an organization can do to break this link.

However, a step that can make it harder, in addition to the efforts to hinder reconnaissance, is keeping systems and their applications patched. Patching reduces the attack surface and makes weaponization more difficult. If target objectives don't provide enough value based on the effort, the threat actor will likely move on to another target.

Delivery, Exploitation, and Installation

After the threat actor creates her exploit kit, she uses one or more lures to get users to deliver her payload. This is the first step in the delivery link, as shown in Figure 3. Lures include email links, Microsoft Office macros included in attachments, links on social networking sites, and DNS redirection to malicious servers.

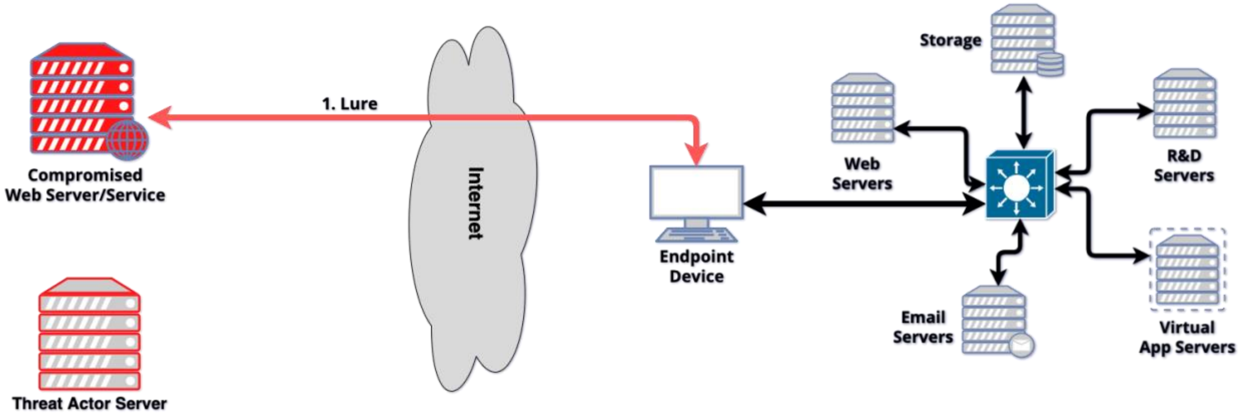

Figure 3: Delivery - Lure

The lure causes the endpoint device to connect to a malicious server to download the exploit kit. In many attacks, a user clicking on a link or opening an infected file causes a drop file to be downloaded and installed. The drop file then calls home to a malicious server and downloads the rest of the attack package. In other cases, the entire attack packet is downloaded and installed: using vulnerabilities to exploit/compromise the device. These steps include the cyber kill chain delivery and installation links, as shown in Figure 4.

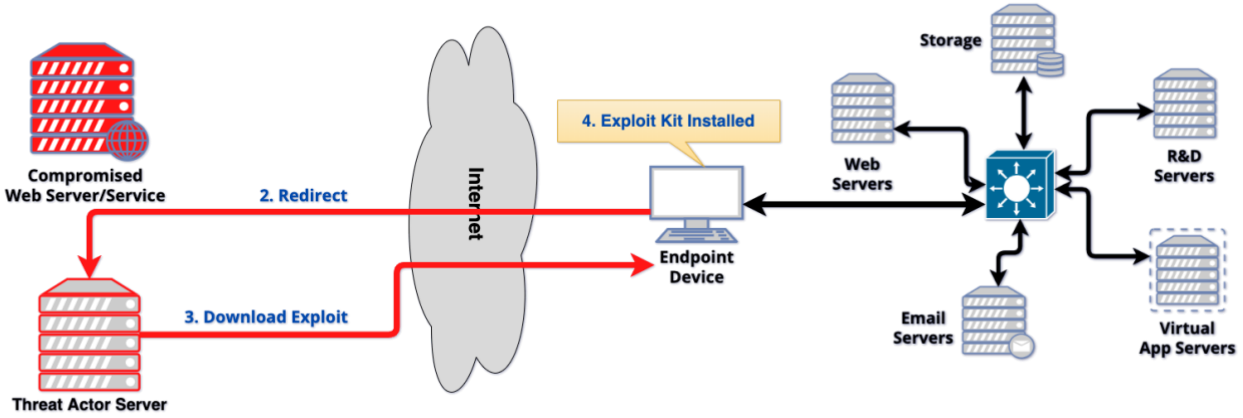

Figure 4: Delivery, Exploitation, and Installation

We can break the delivery and installation links by

- Using antimalware, which is never enough.
- Email filtering and blockage of high-risk attachments.
- Preventing execution of macros not explicitly approved.
- Preventing users from installing any software not specifically in the organization's approved software list.
- Blocking the threat actor’s ability to call back to her server to complete the delivery via web filtering and other tools.
- Ensure that no internal device can directly create an encrypted session, such as HTTPS or TLS, with an external device. This requires a device that intercepts TLS requests from

internal users and then creates an encrypted session between itself and the external device. This allows filtering of all encrypted traffic.

- Train users to not fall for lures.

Several of these safeguards apply across multiple links in the kill chain.

Command and Control

Once the exploit kit is installed, the exploit kit calls home to establish the command and control, or C2, link in the chain. This is how the threat actor provides instructions to the malware and receives data back. C2, as shown in Figure 5, is often encrypted to hide the threat's activities.

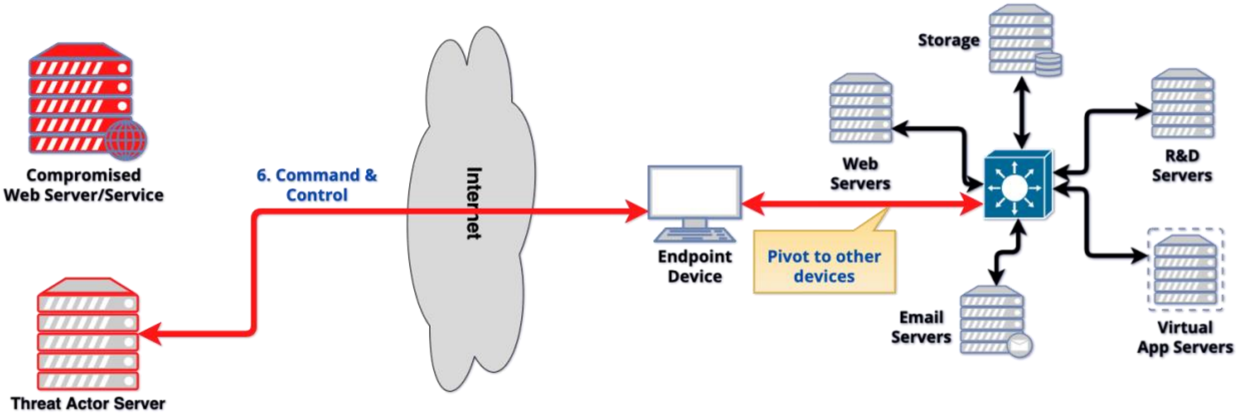

Figure 5: Command and Control

In addition to helping block download and installation of the exploit kit, blocking C2 via web filtering and ensuring the filtering of all encrypted sessions with the outside world is needed. This starts with implementing host-based intrusion detection and firewall solutions.

Actions and Objectives

The final link in the cyber kill chain, Actions and Objectives, can take many forms, including

- Attempts to gain access to high-value targets across the internal network. For this to be effective, the compromised user device must be able to "see" the targets over the network.
- Attempts to gather information from resources the users logged into the device can access or use.
- Attempts to package the stolen data for transmission over the C2 link.

Some of the safeguards already covered can help break this chain. Additional safeguards to break this link include

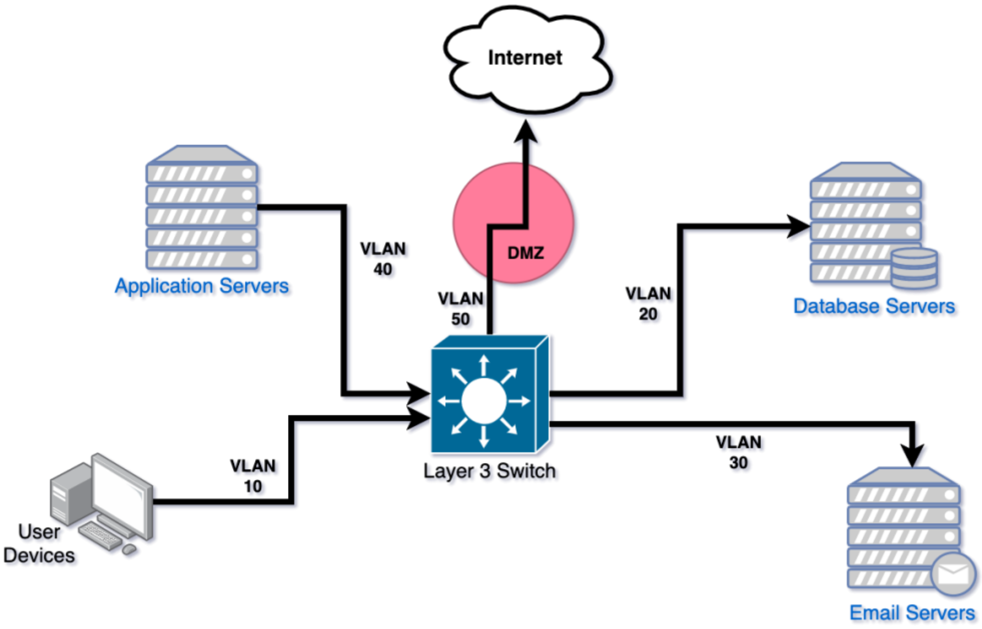

Figure 6: Network Segmentation

- Network segmentation (see Figure 6), including the use of network segment access control lists, helps prevent direct access to databases and other storage of sensitive information.
- Zero-trust networking helps identify anomalous user or device behavior and take steps to manage it.
- Strong authentication for resource access helps prevent threat actors from breaking authentication for access across the enterprise.
- Separation of duties limits what a user can do and what a threat actor can leverage.
- Need-to-know limits what a user can access and, therefore, what a threat actor can see on a compromised device.

Mobile Device Security

The safeguards we've discussed apply to all devices, but mobile devices and servers need additional attention. First, mobile devices.

One of the most significant risks associated with mobile devices is their loss via theft or other means. Many mobile devices contain large amounts of sensitive data. They are also configured to connect via safeguards like certificates. This requires training users on how to maintain control of these devices.

Mobile devices connecting to public networks are at increased risk of compromise. All public networks, both wireless and wired, should be considered hostile. Start with system and network hardening as provided above to mitigate the risk. But more is needed.

Organizations should control what is actually stored on mobile devices. This is easily done by forcing mobile users to access resources via virtual desktops running in the cloud or in the organization's data center. See Figure 7. No data is sent to the remote device except what is shown on the screen. Once the session ends, there are no traces of data on the mobile device.

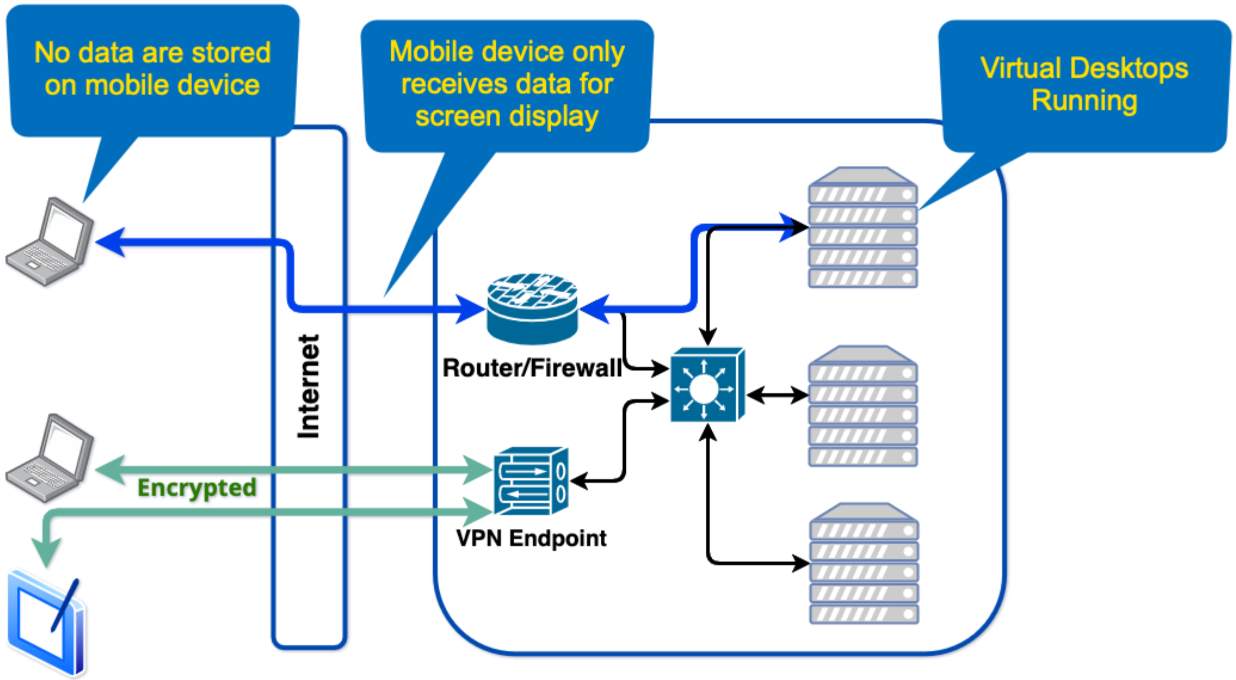
No data are stored on mobile device
Mobile device only receives data for screen display
Virtual Desktops Running
Internet
Router/Firewall
Encrypted
VPN Endpoint

Figure 7: Virtual Desktops

If virtual desktops are not used, the organization should consider using tools designed to help control what is stored locally on remote devices and for how long.

All remote sessions should run over a secure link. The most common approach to this is to use VPN or other implementations of TLS, as shown in Figure 8. Remote devices engage in a handshake with the VPN endpoint to establish an encrypted connection.

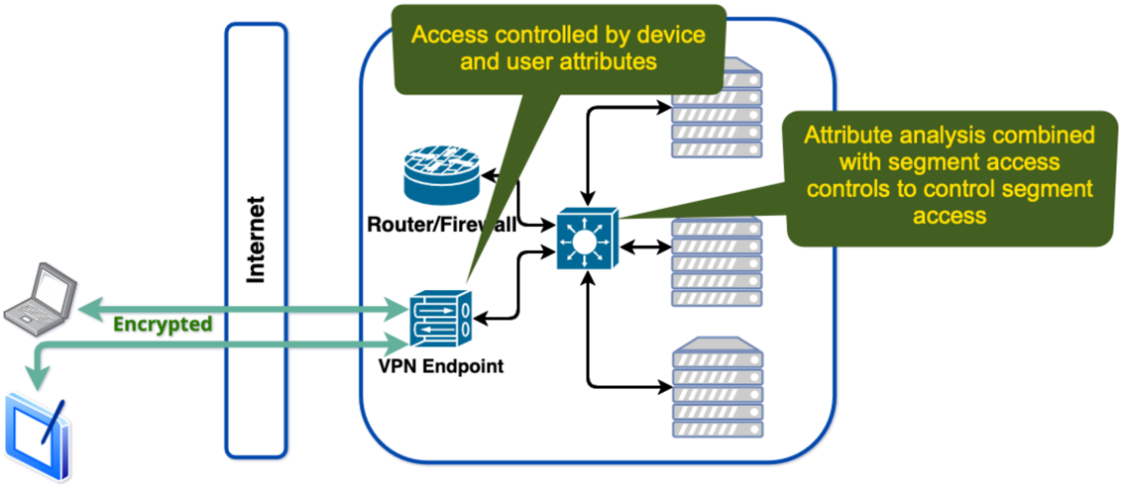
Access controlled by device and user attributes
Attribute analysis combined with segment access controls to control segment access
Internet
Router/Firewall
Encrypted
VPN Endpoint

Figure 8: Mobile Device Access

Access to network resources by mobile devices should be controlled by attribute-based access control and multi-factor authentication: strong authentication.

Attribute-based authentication goes beyond user role assignment. It also looks at characteristics of the entity attempting access, including

- Time of day
- Day of the week
- Location of the device attempting access
- Type of device attempting access
- Resources to be accessed

Full disk encryption of mobile devices helps ensure that a threat actor with physical access to a device cannot gain access. This encryption should be protected with strong user authentication to the device.

Finally, organizations should use a centralized mobile device management (MDM) tool. They range from easy to use and very inexpensive tools, like Microsoft InTune (https://bit.ly/3DFijD9), or a more comprehensive tool, like Mobile Iron (https://bit.ly/3u6NFiQ).

MDM solutions can help manage access and the device policies needed to control the data stored on mobile devices and protect them. Further, MDM provides the ability to wipe a lost device.

MDM and other mobile security considerations are detailed in the NIST special publication 800-124 (Guidelines for Managing the Security of Mobile Devices in the Enterprise, https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final)

Bring Your Own Device (BYOD)

BYOD has grown over the past decade as employees want more flexibility and employers strive to reduce costs. Employees using their own devices can often run their own tools and applications. BYOD also enables easily taking personal applications to the office and business work home. But in addition to general mobile device security, organizations must take additional steps.

The biggest problem with BYOD is increased risk when the organization does not, or cannot, properly manage personal devices that connect to its resources. Figure 9, from the draft of NIST SP 100-22B, *Mobile Device Security: Bring Your Own Device*, details what needs to be considered to manage BYOD risk (Boeckl, et al., 2021)

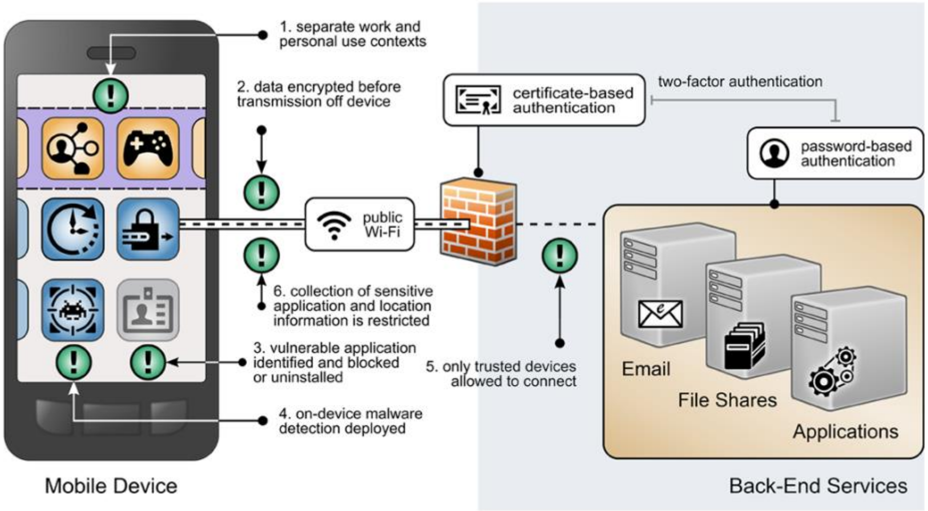
1. separate work and personal use contexts
2. data encrypted before transmission off device
certificate-based authentication
two-factor authentication
password-based authentication
public Wi-Fi
6. collection of sensitive application and location information is restricted
3. vulnerable application identified and blocked or uninstalled
5. only trusted devices allowed to connect
4. on-device malware detection deployed
Email
File Shares
Applications
Mobile Device
Back-End Services

Figure 9: BYOD Security

1. One of the most critical risk management steps is to separate data belonging to the user and those belonging to the organization. This is possible with higher-end MDM solutions. If an MDM is not possible, policies must provide strong control, including periodic audits or data leakage scans, to ensure BYOD devices do not have sensitive data in unexpected locations. One way to manage all of this is to use virtual desktops. Another is to require full disk encryption on all BYOD devices.
2. As with all remote access, all connections to resources must be encrypted.
3. The organization must know if high-risk applications exist on BYOD devices. For devices that access highly classified data, the detection of high-risk applications can result in blocking device access to organization resources. Attribute-based Access Control, ABAC, helps control what devices can connect with what resources. Further, MDM solutions can separate the personal operating context from the business operating context. This ensures that only applications approved by the organization can access sensitive data.
4. All BYOD devices must include antimalware solutions. In addition, host-based firewalls and IDS should be considered.

5. Use of certificates helps to identify approved BYOD devices when they attempt connections. Combined with user multi-factor authentication and ABAC, this helps ensure only expected and managed devices connect.
6. MDM tools can track what applications are installed, data stored, and the locations from which devices attempt to connect. However, there is a boundary between user privacy and organization risk management. This boundary shifts based on the user's role, the classification of data accessed, and the categorization of resources used. In many cases, BYOD may introduce more risk than management is willing to accept.

Server Hardening

Finally, let's look at server hardening. Each server requires a general set of hardening steps and risk-based hardening steps.

General Hardening Steps

General hardening steps apply to all servers, including

- Keep the OS patched and up-to-date.
- Ensure only required applications are running
- Disable the use of browsers
- Block direct internet access for servers not providing web services
- Use strong authentication
- Use strong password and account policies
- Disable USB ports
- Use full disk encryption where appropriate
- Use secure firmware, like Intel's platform firmware resilience (https://bit.ly/3uX9Nve)
- Use Confidential Computing technology (https://bit.ly/3r3qYtN)

In general, each server should perform a specific role. Only applications and tools that support that role should run. This is easily done when using virtual servers and operating systems configured only for that role, as with Microsoft server implementations (Microsoft, 2021).

Another consideration is not to mix data of different classifications on the same server. For example, we should not place confidential data on the same server as top-secret data. Mixing includes data that are processed, pass through, or stored on a server.

Risk-based Hardening Steps

Each server runs one or more applications. These applications, and supporting tools, require special attention that likely requires risk-based considerations for hardening, including

- Check for vulnerabilities daily and ensure vendors manage these effectively.
- Patch or upgrade as needed
- Segment application servers from databases servers and control access at the network level

- Monitor and control changes to applications
- Monitor and control installation of applications
- Audit application use
- Use multi-factor authentication for applications when risk dictates
- Monitor and control activity with network- and host-based IDS/IPS
- Use one or more antimalware layers based on risk

Final Thoughts

As with all security safeguards, managing endpoint security is about managing risk. While there are essential safeguards that all organizations should implement, there are also specific steps each organization must consider when assessing its susceptibility to attack.

The cyber kill chain helps organizations understand how endpoint devices are compromised. It enables processes for assessing risk unique to each endpoint device set.

OSINT is an excellent way to determine what a threat actor can find out about an organization via passive reconnaissance. Sanitizing OSINT as much as possible and then taking steps to minimize what is publicly available are crucial elements of reconnaissance defense.

Works Cited

Boeckl, K., Grayson, N., Howell, G., Lefkovitz, N., Ajmo, J. G., McGinnis, M., . . . Ward, P. (2021, March). *Mobile Device Security: Bring Your Own Device NIST SP 1800-22 Practice Guide Draft*. Retrieved April 2022, from NCCoE: https://www.nccoe.nist.gov/publications/practice-guide/mobile-device-security-bring-your-own-device-nist-sp-1800-22-draft

Lockheed Martin. (2022). *Proactively Detect Persistent Threats*. Retrieved April 2022, from Lockheed Martin: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Microsoft. (2021, July). *Install or Uninstall Roles, Role Services, or Features*. Retrieved April 2022, from Microsoft Docs: https://docs.microsoft.com/en-us/windows-server/administration/server-manager/install-or-uninstall-roles-role-services-or-features

Olzak, T. (2020, July). *Open Source Intelligence for Cyber Offense and Defense*. Retrieved April 2022, from Toolbox: https://www.toolbox.com/tech/devops/videos/open-source-intelligence-for-cyber-offense-and-defense/

Zola, A. (2021). *Footprinting*. Retrieved April 2022, from TechTarget: https://www.techtarget.com/searchsecurity/definition/footprinting