Preventative Measures: Attachment Filtering

This lesson will briefly cover what attachment filtering is, and why it's used. One way to stop malware landing in employee mailboxes is by limiting what types of files are allowed to come into the organization as email attachments. There are many tools out there that offer this functionality, but we will cover generally how these tools operate, and why this can be a good preventative security control.

FILTERING

It isn't a good idea to block attachments outright – employees will have difficulty sending legitimate documents internally and externally. The most appropriate way to approach this situation is to consider what file types are often used for malicious purposes, which file types the organization deals with on a regular basis, and whether blocking them would have any negative impact on the business. The most obvious file types that are used for malicious activity are:

- **.exe** (Executable)
- **.vbs** (Visual Basic Script)
- **.js** (JavaScript)
- **.iso** (Optical Disk Image)
- **.bat** (Windows Batch File)
- **.ps/.ps1** (PowerShell Scripts)
- **.htm/.html** (Web Pages / Hypertext Markup Language)

Typically businesses will use and send the following file formats via email, which can also be used for malicious purposes:

- **.zip** (Archive)
- **.doc/.docx/.docm** (Document file, often for Microsoft Word)
- **.pdf** (Portable Document Format)
- **.xls/.xlsx/.xlsm** (Spreadsheet file, often for Microsoft Excel)

Email gateways and email security tools will often allow for different actions to be taken once a certain attachment has been identified, such as scanning it for malicious indicators, blocking the email from being delivered, quarantining the email, stripping the attachment, alerting the email gateway administrator, sending an email to specific recipients about the activity (such as the security team), or generating logs which can be ingested by a SIEM platform and used to generate an alert for security analysts to investigate.