CYBERRISKS&LIABILITIES

Man-in-the-Middle Cyberattacks Explained

A man-in-the-middle (MITM) cyberattack refers to a cybercriminal intercepting a digital interaction or exchange between individuals, systems or an individual and a system. During a MITM incident, a cybercriminal could either eavesdrop on an interaction or pretend to be a genuine participant in the exchange. MITM cyberattacks leverage various strategies to manipulate targets, but the goal of these incidents is largely the same—to retrieve confidential data (e.g., banking details or login credentials) and use it to commit additional crimes, such as identity theft or fraudulent fund transfers.

Although individuals are targeted in MITM cyberattacks, such incidents are also a pressing concern for businesses. After all, cybercriminals may utilize individuals' stolen data to compromise their workplace technology and assets (e.g., customer information, intellectual property and company funds), potentially resulting in significant losses and business disruptions. With this in mind, it's vital for businesses to take steps to safeguard their operations and employees against MITM incidents.

This article provides more information on MITM cyberattacks, outlines examples of such incidents and offers prevention measures for businesses to consider.

MITM Cyberattacks Explained

A MITM incident typically occurs in two phases. These phases include interception and decryption. During the interception phase, a cybercriminal will attempt to gain access to their target's technology—usually via a poorly secured Wi-Fi router or fake hotspot—and interfere with the victim's network connection. From there, the cybercriminal will be able to insert themselves between any digital interactions or exchanges their target may have, thus establishing themselves as the "man in the middle." As a result, the cybercriminal will have the ability to collect any confidential data shared during their target's interactions or exchanges (unbeknownst to the victim).

During the decryption phase, the cybercriminal will decode any data they collected from their target, therefore making this information intelligible and allowing it to be utilized to commit further nefarious acts. Cybercriminals may implement a range of techniques to carry out MITM incidents, including the following:

- **Internet protocol (IP) spoofing**—Any technology with a Wi-Fi connection has a designated IP address that allows for communication with other connected devices or networks. When a cybercriminal engages in IP spoofing, they alter IP address characteristics to mimic their target's technology system, ultimately sending the victim to fraudulent websites where they may unknowingly share their data.
- **Domain Name System (DNS) spoofing**—This tactic entails a cybercriminal changing elements of a target's DNS server as a way of redirecting the victim's online traffic to fake websites that closely resemble intended domains. If the target logs in to any of these false websites, they will have unintentionally provided the cybercriminal with account credentials and associated data.
- **HTTPS spoofing**—HTTPS is an internet communication safeguard intended to preserve data confidentiality between an individual's device and the websites they browse. Through HTTPS spoofing, however, a cybercriminal tricks their target's browser into thinking a malicious website is safe and secure, thus allowing the victim to access it and unwittingly share their data.

- **Secure sockets layer (SSL) hijacking**—An SSL certificate is a digital authorization intended to authenticate a website's identity and ensure an encrypted connection. When browsing, most devices automatically reroute individuals from unsecured websites to those with SSL certificates. During SSL hijacking, a cybercriminal uses their own technology to intercept this reroute, halting any information passed between their target's device and web server. Afterward, the cybercriminal will gain access to any data the victim shares for the remainder of their browsing session.
- **Email hijacking**—This tactic involves a cybercriminal infiltrating a target's email account, monitoring their conversations and collecting any data they may find within these interactions. Furthermore, this tactic may lead to the cybercriminal impersonating the victim via email and launching phishing scams against other associated parties (e.g., co-workers, customers or vendors) to gain access to additional data or conduct fraudulent fund transfers.
- **Wi-Fi eavesdropping**—Wi-Fi eavesdropping is when a cybercriminal creates a fraudulent public Wi-Fi connection with a seemingly genuine name, such as that of a nearby business. If a target connects to this Wi-Fi, the cybercriminal will then be able to monitor the victim's online activity and gather any data they share while connected.
- **Browser cookie theft**—A browser cookie is a piece of personal information that a website maintains on an individual's device, such as payment card details or login credentials. If a cybercriminal is able to infiltrate a target's device, they may also gain access to its browser cookies, compromising the victim's data.

Examples of MITM Cyberattacks

A variety of large-scale MITM incidents have occurred in recent years. In 2015, IT experts discovered that a malicious program known as Superfish had been pre-installed on technology company Lenovo's devices since 2014, affecting numerous individuals. This program utilized SSL hijacking tactics to permit cybercriminals to interfere with victims' secure browsing sessions, direct them to fraudulent websites and even place harmful advertisements within encrypted domains.

In 2017, several financial institutions identified security vulnerabilities within their mobile banking applications that had contributed to MITM incidents among customers with iOS and Android phones. These vulnerabilities failed to uphold proper online hostname verification techniques, allowing cybercriminals to use false SSL certificates to bypass internet security protocols and conduct MITM cyberattacks.

Altogether, these real-world examples highlight how crucial it is for businesses to implement effective measures aimed at preventing MITM cyberattacks.

MITM Cyberattack Prevention Measures

To help avoid and minimize the impact of MITM incidents, businesses should consider utilizing these measures:

- Train employees on safe internet browsing measures, including how to ensure a secure connection and detect potentially fraudulent websites.
- Establish a virtual private connection (VPN) for employees to use for all work-related internet browsing. Prohibit employees from utilizing public Wi-Fi connections.
- Require employees to create complex and unique account passwords, as well as update these passwords on a routine basis.
- Implement multifactor authentication capabilities on all workplace technology. Only provide employees with access to sensitive data if they need it for their specific job duties.
- Encrypt sensitive company data. Conduct frequent data backups of any critical information in a safe and secure location.
- Equip workplace technology with sufficient security software (e.g., antivirus programs, firewalls and endpoint detection tools). Update this software as needed to ensure effectiveness.

- Keep workplace networks properly segmented to help contain potential MITM cyberattacks and limit associated damages.
- Purchase adequate cyber insurance for protection against losses that may result from MITM cyberattacks. Consult a trusted insurance professional to discuss specific coverage needs.

Conclusion

As a whole, it's evident that MITM incidents pose significant cybersecurity threats and data protection concerns for all businesses. Yet, by having a better understanding of this cyberattack method and implementing sufficient prevention measures, businesses can help keep MITM risks at bay.

For more risk management guidance, contact us today.