Top 5 Data Security and Privacy Trends Revealed by Feds – and 5 Proactive Steps Employers Can Take Today

Insights
2.15.22

The United States Cybersecurity & Infrastructure Security Agency (CISA) recently issued a Joint Advisory providing an overview of 2021 ransomware trends, noting several key developments that employers should take note of. The February 9 Advisory was prepared jointly with cybersecurity authorities from the United Kingdom and Australia, which emphasizes the global threat of ransomware. This Insight reviews the top five trends contained in the Advisory, and provides the top five proactive steps employers can take to reduce your risk.

Top 5 Data Security and Workplace Privacy Trends

1. **Top Attacks:** Attackers continued to gain access to company networks by using phishing emails and exploiting Remote Desktop Protocol (RDP) as well as software vulnerabilities.
2. **Smaller Businesses, Beware:** The Advisory warned of increased attacks on smaller-sized businesses. This comes after several high-profile infiltrations targeting the nation's food and energy supply chains resulted in security crackdowns at larger organizations.
3. **Triple Threat:** CISA observed a rise in "triple extortions." Previously, attackers would only seek to block access to company networks, demanding ransom in exchange for regaining access. Over time, attackers started to threaten the release of stolen, confidential information to the public in addition to blocking access ("double extortion"), as companies started creating better backups to protect their data. Recently, the tactics have evolved to include threats to inform companies' partners, shareholders, or suppliers about the attack – a third level to the extortion schemes.
4. **Magnification Danger:** The Advisory found that ransomware groups sought to magnify damage in several ways. They have targeted cloud accounts and cloud-based data backup and storage systems. Attacks on managed service providers (MSPs) were also on the rise – this is particularly dangerous because MSPs provide network and infrastructure support to companies who often do not have the resources to perform them in house. By nature, MSPs have access to the networks of many companies, so an attack on a single MSP could cause widespread collateral damage.
5. **Cybersecurity Needs to be 24/7:** Finally, CISA advised companies to be vigilant about ransomware attacks during holidays and weekends, given that many employees and outside security professionals are not at work during those times.

Top 5 Proactive Steps for Employers to Deploy

Given this information, there are multiple steps employers can take to mitigate ransomware attacks. Here are the top five steps you can take to minimize the danger.

1. **Stay Up to Date With Patches:** CISA notes that regularly patching software is one of the most efficient and cost-effective ways to prevent attacks. New software vulnerabilities are constantly being discovered, and software companies are continuously releasing updates to patch them. For instance, Microsoft just released software updates to patch four dozen potential vulnerabilities on February 8.
2. **Maintain Remote Access Vigilance:** Given that many employees are still working remotely at least part-time, CISA emphasizes the need to monitor their remote access. This includes observing RDP usage, such as log-in locations and number of log-in attempts.
3. **Disable Credentials Upon Departure:** It is also highly important to ensure that RDP credentials are immediately disabled once an employee leaves the company or otherwise no longer needs the credentials. This is especially true in today's high-turnover business environment. Indeed, many ransomware attacks in 2021 occurred because of compromised or outdated RDP credentials.
4. **Deploy Multifactor Authentication:** Adding an extra layer of security is never a bad a thing. Consider requiring multifactor authentication for employees to gain access to company networks.
5. **Consider Other Mitigation Efforts:** Other steps you can take to put yourself in the best position in today's environment include offering regular – and practical – cybersecurity training to your workforce and creating data backups with regularity.

Conclusion

Fisher Phillips will continue to monitor further developments in these areas, so be sure to subscribe to Fisher Phillips' Insight system to stay up-to-date. If you have any questions regarding how your organization can mitigate the risk or ransomware attacks, please consult your Fisher Phillips attorney, the author of this Insight, or a member of Fisher Phillips' Privacy and Cyber Practice Group.

Service Focus

Privacy and Cyber