Not If But When: Cybercrime Targets Telework

Insights
10.02.20

As a result of the COVID-19 pandemic, millions of Americans have deserted the physical workplace. Modern technology and remote access capabilities have made it possible to transform almost any job to a telework position. As the initial scramble to remote work becomes the norm, you should revamp telework and cybersecurity policies to combat increased cybercrime targeting employees working from home.

Background Information: The Problem Is Real
Since the historic shift to telework, the FBI has reported a 400% increase in the number of cyberattack complaints reported to the Department's Internet Crime Complaint Center. Interpol has released a Cybercrime COVID-19 Impact Report finding that cybercriminals have shifted their focus from targeting individuals and small businesses to targeting major corporations, governments, and critical infrastructure. The United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, and the United Kingdom's National Cyber Security Center issued an alert warning that cybercriminals are exploiting COVID-19 to conduct cybercrime.

Cybercriminals have used COVID-19-related themes to target victims. Both the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC) have warned that cybercriminals are using phishing emails purported to be from them to steal data from unsuspecting recipients. In addition to targeting vulnerable telework networks, cybercriminals are manipulating heightened emotions like fear and anxiety to engage in a variety of destructive cybercrime.

The full scope of the damage of cybercrime is unknown because many corporate victims prefer to keep cyberattacks private. However, those examples that become public are staggering. In late July, it was revealed that a large corporation paid $4.5 million to cybercriminals for the return of data compromised by a ransomware attack. Local governments in Alabama and California have made headlines for similar bad fortune. Unfortunately, one thing is clear – the rushed and historic shift to telework left holes in cybersecurity systems that criminals are willing and eager to exploit.

How Do Cybercriminals Commit Cybercrime?
There are some common ways in which you might find your workplace subject to a cyber-attack.

Phishing And Spear Phishing

Phishing emails are a tool used by cybercriminals to collect private data from unsuspecting victims. Phishing scams typically target hundreds or thousands of victims at a time by sending a spoofed email claiming to be from a reputable entity asking that the victim share personal information directly with a cybercriminal.

Spear phishing is a targeted form of phishing. It has become a common tool for cybercriminals who target businesses. Spear phishing emails can be difficult for employees to identify because the cybercriminal will research the recipient to create an authentic-seeming email. Ordinarily this involves spoofing an email from the recipient's supervisor or manager. Sophisticated employers are hyper-aware of spear phishing threats and, in most cases, train their employees how to identify and report such threats.

Business Email Compromise (BEC)

A BEC is the type of cyberattack that occurs when a cybercriminal poses as a company employee with the goal of convincing another employee to share confidential or sensitive information or to perform a task requested by the cybercriminal. These attacks are usually carried out using a spear phishing email. A typical BEC scam involves the cybercriminal creating an email that looks like it was sent from a high-level executive within the company. The email will typically claim that some emergency requires the employee take immediate action or provide confidential information. The employee, believing that they are corresponding with the real company executive, grants the request.

The above scenario may sound too simple to be of great threat to your company but trust us – it isn't. The FBI has categorized BECs as one of the most financially damaging cybercrimes. According to a recent FBI Public Service Announcement, BECs were responsible for more than $2 billion dollars in theft from businesses between 2014 and 2019.

Ransomware Attacks

Ransomware is a type of malicious software that can prevent a company from accessing its own networks or data. Cybercriminals use ransomware to hold a company's data hostage until the company pays a ransom for its return – hence the clever moniker. Ransomware attacks cause expensive disruptions and can result in the loss and theft of private data. Cybercriminals often gain access to a business's network using a spear phishing email. The spear phishing email will contain a link or an attachment, which, if accessed, acts as a portal for cybercriminals to gain access to your company's network.

Even more concerning than the possibility of being held ransom by a cybercriminal is a new and disturbing evolution of ransomware called "doxware." A doxware attack occurs when a cybercriminal steals a company's data and threatens to sell it and inform the media or the company's customers that the data was compromised and sold unless the victim pays a ransom. Failure to pay the ransom in a doxware situation could result in permanent and irreparable damage to a company's reputation.

Preventing Cybercrime

Now that the dust has settled from the initial shift to telework, you should take the time to re-visit cybersecurity policies and to refresh employees' memory of the same. The clear majority of cyberattacks all have one thing in common – they require a company employee to open the door for the attack. In this instance it is helpful to think of cybercrime as a burglary. Just as you would train employees to prevent a burglary by locking the doors or setting an alarm before leaving the building, you should train them to prevent cybercriminals from gaining access to your network.

Train Employees to Prevent Access

The single-most important tool for preventing cyberattacks is a well-educated staff. Training provided to employees should include a brief explanation of the various tools cybercriminals use to engage in cybercrime and tips for identifying spear phishing emails.

You should train employees to be wary of any request that is accompanied by a sense of urgency. Company policy should encourage employees to seek confirmation for any suspicious or urgent requests that are made without prior notice. You should expect that cybercriminals will create spear phishing emails claiming to be from high-level company officers, often for a wire transfer, or requesting W-2 data or other sensitive personal or company information. Because of this, company policy should reinforce that seeking confirmation for a request from a high-level company employee will not result in disciplinary action.

You should notify employees that cybercriminals may try to target those who are teleworking during the pandemic. In addition, they may try to capitalize on the pandemic to entice employees to provide confidential information or download ransomware. Emails containing COVID-19 updates or information are a popular lure for phishing and spear phishing emails. However, COVID-19 is not the only subject cybercriminals use to lure unsuspecting employees. You should train employees to evaluate any emails containing urgency, playing on emotion, or emphasizing the secrecy of transmission of funds or sensitive information.

Enact Comprehensive Cybersecurity Policies

If not already in place, you should draft telework cybersecurity policies to address the enhanced risk that telework poses to your organization. Among other things, these policies should address the use of personal-devices for telework, communication standards for the company, the use of non-secured public Wi-Fi for telework, and reporting requirements for suspicious activity.

Maintain Adequate Security

You should work with your IT staff to ensure that remote access technologies are current and secure. Your IT department should closely monitor cybercrime trends like which lures are popular and what software is vulnerable to cyberattacks. IT should create a logging system capable of tracking a cyberattack if your network becomes compromised. IT departments need to remain vigilant, updating cybersecurity policies as necessary to ensure maximum security. Finally, you should devise a procedure for responding to security compromises.

Conclusion

Multiple reports confirm that cybercriminals are targeting telework. You should treat the possibility of a cyberattack as a "not if but when" scenario. If your employees have not already been the target of a spear phishing attack while teleworking, they will be.

Security measures that may have been appropriate at the beginning of the pandemic could now be outdated and leave your network vulnerable to potential compromise. Updating or creating comprehensive cybersecurity policies and training employees to spot potential cyberattacks may save your company significant costs and loss of reputation.

For more information, contact the authors here or here.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Service Focus

Privacy and Cyber

Litigation and Trials

Counseling and Advice