McCloskey Partners, LLC
http://www.mccloskeypartners.com/
11.24.2015

Cyber Attacks are on the Rise—Is Your Network Secure? Are your HR Policies ready for a Cyber Attack?

In early November, a group of hackers took aim at global financial interests and Cloud providers of secure email and office suite services. As the number of malicious and data-theft hacks rise—how do you know your company network is secure?

While cyber attacks are launched every day, the recent hack on Zoho, a Cloud provider of online business tools, brought the company to a halt. The Zoho attack was part of a larger attack on Swiss and Thai financial firms, and other email providers. Zoho, and other software as a service (SaaS) companies, were threatened with attack unless a ransom was paid.

For one email service, ProtonMail, the severe attack was too much for their internet service provider (ISP), who encouraged ProtonMail to pay the demanded $6,000 bitcoin ransom—which they did. Created by scientists at CERN, the European organization for nuclear research, ProtonMail is an encrypted email service intended to protect the private communications of activists, journalists, scientists, and others, from electronic spying by individuals and nation states.

Both ProtonMail and Zoho took the unusual step of speaking up about the ongoing attacks, keeping their users informed. Oftentimes, victims of DDoS and data theft keep the intrusion—and payment of ransom—quiet.

Despite paying the ransom, attacks against ProtonMail continued, leading the organization to state, "This was clearly a wrong decision so let us be clear to all future attackers – ProtonMail will NEVER pay another ransom."

The group behind the large attack on these companies and services is purportedly called the *Armada Collective*. Prior to attack on their target, the hackers sent a message that read in part:

"All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins. When we say all, we mean all - users will not be able to access sites host with you at all. If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time. Bitcoin is anonymous, nobody will ever know you cooperated."

Other email services like Neomailbox, Runbox, and Hushmail were attacked after refusing to pay ransom.

Could this happen to your company?

Distributed denial of service (DDoS) is a common form of cyber crime. For reasons of malice, or money, DDoS attacks aim compromised computers, called botnets, at a target website or network, where the target is overwhelmed and shut down by the traffic.

While DDoS attacks are overt and damaging, other intrusions cost your company time, money, and reputation, including:

- **Unwanted advertisements, tracking, and pop-ups:** Free software is often accompanied by adware and spyware. Spyware can open a door for device takeover, or lead to slow performance and frequent pop-up windows.
- **Reconfiguring:** Desktop and mobile devices can be reconfigured by viral and other threats. When a device is controlled remotely, it could become part of a botnet used to attack others.
- **Trojan, DDoS and data theft:** Direct hacks, hacks through misappropriated passwords, and data theft often occur with a DDoS.

Incapsula, a secure, Cloud-based delivery platform, estimates DDoS attacks can cost $40,000 per hour in lost service, sales, consumer confidence, and company function. Among other business departments, IT, HR, and customer service suffer financial and other impacts during and after a DDoS attack.

Prepare for cyber intrusion now

Also in November, indictments were handed down for what was described by U.S. Attorney General Loretta Lynch as "one of the largest thefts of financial-related data in history."

Describing the attack on JP Morgan Chase as "hacking as a business model," United States Attorney for the Southern District of New York, Preet Bharara stated, "Companies need to do a better job of protecting all the information that they have because even information like email addresses, and location information, can be used for devious purposes, to the detriment of a lot of people who were their customers."

The message is clear and the loss is real. Business continuity planning helps your business identify risk, deter attack, and manage cyber intrusion when it happens. HR is a natural leader to drive development of cybersecurity best practices in any organization or business. When you need experienced counsel with HR best-practices, speak with our firm.

Contact McCloskey Partners, LLC today to discuss your Cyber Policy at 215-716-3035 or admin@mccloskeypartners.com