AMERICAN HEALTH LAW ASSOCIATION

COVID-19 Cyber Attacks: Ten Tips for Health Care and Other Organizations

June 05, 2020

Saad Gul, Poyner Spruill LLP

Mike Slipsky, Poyner Spruill LLP

The U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has warned of escalating cyber attacks on organizations working on the COVID-19 pandemic. CISA, the Federal Bureau of Investigation, and the British government have all warned that the attackers are seeking to exploit the pandemic. Among those targeted are medical researchers, government entities, academics, pharmaceutical corporations, and research facilities.

The attacks are prompted by a desire to seek, exploit, and potentially monetize COVID-19 research. Global companies and their vendors are particularly vulnerable. They are often seen as the soft underbelly that allows access to key data. The increase in remote work has further weakened defenses.

The attacks themselves use a familiar playbook. Old phishing techniques remain popular. Unfortunately, they are popular because they work. The target has to thwart each incursion. The attacker only has to get lucky once. Attackers also use known vulnerabilities in networking and security software to access data.

While the remedies are simple, organizations must repeatedly remind and drill personnel to use them. Here are the top ten suggestions for organizations.

First, consider flagging all incoming messages that originate outside your organization. The minimal nudge the flag provides could be all that most employees need to approach their mail with caution.

Second, keep all software, systems and hardware current. Install security updates consistently and regularly. This is important because many attackers reverse-engineer software patches to identify the problem the patch remedies. If the patch is not applied, your system has a known vulnerability, and no defense against it.

Third, draft and enforce procedures for remote meetings. Zoom, Webex, Microsoft Teams, and similar software has become indispensable in the past few months. Consistent policies and procedures for their use, such as mandating a password requirement, are low-cost- high-yield measures.

Fourth, require secure passwords. Easily guessed passwords such as the name of the company should be avoided. Contrary to prevailing belief, we do not necessarily recommend mandating frequent password changes. Frequent changes lead employees to use simpler passwords. The organization may well be better off with a complex password less vulnerable to attack. This should be coupled with multi-factor authentication. Multi-factor authentication ensures that even a compromised password will not entail a breach in the system.

Fifth, provide IT with the capacity to track activities on the system: logging capabilities. These are invaluable in detecting intrusions. If a breach does take place, it enables the organization to assess the damage. An accurate assessment of damage reassures clients, regulators, and eases recovery. And it ensures a more robust defense in the future.

Sixth, a disproportionate number of attacks originate from a handful of dubious domains. CISA recommends automatically barring all communication with these known domains. This is a one-time measure every organization should implement. Doing so frees up human and technical resources to tackle other threats.

Seven, phishing has remained a persistent threat for one reason. It works. The playbook is well known. It involves a message from a high-ranking official, urgently seeking critical information, with a tight timeframe. The recipient is warned that failure to comply will lead to catastrophe. This process combines several psychological vulnerabilities. Warn your employees to watch out for them. And run regular drills so that they become familiar with the scam. The more familiar they are, the easier it is to spot it “in the wild.”

Eight, if your IT infrastructure is old, and therefore vulnerable, consider reinforcing available defenses. Everything from firewalls to antivirus software bolsters overall security. The objective is not to become impervious to attack. That will never happen. But it makes the organization a harder target. This offers two advantages—attackers will take their business elsewhere and if a breach occurs, the organization can establish its commitment to security to regulators investigating the incident. Regulators do not expect perfection. They do expect, however, a minimal level of effort.

Nine, have critical information, including architecture and contact details available on paper and accessible. One of our favorite movies, Dr. Strangelove, includes a scene where U.S. President Mufflin and Soviet Premier Kissoff are trying to avert nuclear war. This requires contacting the “People’s Air Defense Center” in Omsk. When Mufflin asks for the number, the hapless Kissoff can only suggest trying Omsk information. Ensure that the organization has access to its version of the critical Omsk number. If a significant attack cripples the organization’s computer network, it can assemble the team and address the crisis without losing precious time tracing people without electronic directories.

Ten, regularly review and update the organization’s incident-management plan. The plan should detail who will do what in the most likely attack scenarios that will confront the organization. The regular review is necessary because organizations rarely revisit the plans after the initial draft. Circumstances change. For instance, large-scale remote work was largely unknown till March.

Saad Gul and **Mike Slipsky** are partners with Poyner Spruill LLP. They advise clients on a wide range of privacy, and cybersecurity issues, including HIPAA, GDPR, FERPA, CCPA, and other privacy regimes. Saad (@NC_Cyberlaw) may be reached at 919.783.1170 or sgul@poynerspruill.com. Mike may be reached at 919.783.2851 or mslipsky@poynerspruill.com.

.