HURON

Covid-19: Critical Cybersecurity Actions for Healthcare Organizations

Amid the COVID-19 pandemic, cybercriminals are showing no restraint in exploiting turmoil surrounding the coronavirus. Attempts to attack the World Health Organization have doubled, a COVID-19 vaccine testing facility was the victim of an attempted ransomware attack, and other known phishing and ransomware campaigns are using the coronavirus pandemic to actively target healthcare workers.

Attacks that would be debilitating during times of normal business operations could be catastrophic for organizations and patients batting COVID-19.

Below are immediate actions organizations can take to thwart cyberattacks and remain focused on providing care and services to consumers:

Utilize phishing simulation security awareness trainings.

Leaders can expect to see a continued uptick in coronavirus-related scams and phishing emails directed at their employees.

As organizations move more of their workforce to virtual work environments, employees are having to quickly adapt to new technology in challenging settings. Many are using personally owned equipment that has not been properly provisioned against security attacks. These challenges make end users especially vulnerable to phishing campaigns, as people contend with the personal distractions and increased professional workloads brought on by COVID-19.

The most important defense against phishing and other social engineering attacks is training. Employees should be trained to recognize and protect themselves against the subtle clues and traits of phishing attempts, including misspellings, poor grammar, alarmism and requests to divulge any information that is sensitive, such as passwords.

Phishing simulations are the most effective way to train workforce members to recognize and take appropriate action when they encounter fake or phishing emails. During phishing simulations, organizations send deceptive emails to staff to gauge workforce response and the ability to recognize malicious emails. The simulations enable organizations to identify employees who may be susceptible to attacks and provide further training.

Deploy two-factor authentication.

In order to transition to a remote workforce, access to corporate network resources is often required. To facilitate this move, access needs to be granted in such a way that secures information while granting appropriate access. This is usually achieved using a virtual private network (VPN) connection to the network or through using virtual access tools like remote desktop protocol (RDP).

Cybersecurity best practices strongly recommend that remote access be facilitated using two-factor authentication in addition to using strong, unique passwords. For a network that is not properly segmented, a compromised VPN connection can give a malicious user nearly unlimited access to network resources and sensitive data. Two-factor authentication requires a second step to confirm the identity of the user prior to access being granted. The second step may be a code sent via text message to the user's phone or the use of an authentication application. In addition to two-factor authentication, VPN software should be updated with the latest security patches and include enough licenses to support the organization.

Accelerate a move to the cloud.

The infrastructure and network or internet connections supporting cloud applications have proven extremely reliable and robust amid the disruption of COVID-19. For example, cloud teleconferencing vendor Zoom has been able to effectively scale its services in a matter of days as schools and businesses moved their operations online.

To adjust to larger remote operations, some organizations might be required to drastically increase the number of licenses for technical tools and capabilities. In some cases, a move to cloud applications may be less expensive and provide better, more robust alternatives to more licenses for on-premise applications.

Accelerating the move to the cloud for enterprise systems or hospital information systems may be constrained by vendor timeframes or an organization's availability of resources and staff. However, moving to cloud applications for backoffice or administrative applications such as to Microsoft Office 365 should be achievable. Additionally, more narrowly focused or niche applications may be worth considering for movement to the cloud.

Implement, enhance and expand telehealth capabilities.

COVID-19 has hastened the need for organizations to offer or expand telehealth capabilities. Prior telehealth implementations focused on highly tailored solutions for distinct or narrow patient populations. Now organizations are turning to telehealth and virtual care options to maintain regular services and deliver immediate COVID-19 responses.

The Office for Civil Rights (OCR) has removed one of the major challenges to the rapid deployment of telehealth capabilities, which is the suspension of enforcement actions requiring that telehealth vendors be business associates of the provider or have a signed business associate agreement in place. The temporary suspension allows the use of any tele-video technology for any clinical purpose, not just for diagnosis and treatment of illnesses related to COVID-19 related.

As organizations expand telehealth, best practices should be maintained for protecting patient data, obtaining patient consent, communicating with payors regarding qualified payments and deploying appropriate levels of cybersecurity.

For more information, contact us or visit our COVID-19 resources page.

HURON

huronconsultinggroup.com