Akamai

PAPER

Cybersecurity for Healthcare Providers

Introduction

To compete in a fast-changing market, healthcare provider organizations adopt new devices and applications to provide premium patient care and next-level experiences. Each new addition brings its own benefits to patients — and its own set of security risks to the organization.

This complex IT environment, combined with the high value of protected health information (PHI), creates an irresistible opportunity for cybercriminals, who continue to pummel systems. According to a U.S. Department of Health and Human Services report and research by IBM, the healthcare industry has seen a 50% increase in cyberattacks since the onset of the pandemic, and those attacks were the most expensive, with an average cost of $7.13 million per incident. That IBM report highlighted that ransomware attacks were the most common threat — as malicious actors preyed on the need for hospital and healthcare systems to be restored quickly — followed by data theft and server access. Healthcare providers, in particular, are attractive ransomware targets because electronic health records (EHRs) can go for $1,000 each on the dark web, compared with credit card information for approximately $110 and Social Security numbers for a mere $1 each.

With a constantly growing number of threats against their systems, many organizations are not adequately prepared to mitigate them. Worse, some have already been infiltrated and don't know it. Threat actors may already be exfiltrating data or waiting for the right moment to strike.

Now is the time to gain clarity on your organization's attack surface by taking an inventory of devices and how they connect to your infrastructure. With better knowledge of where vulnerabilities exist, putting a sound mitigation plan in place will prevent or minimize the potential impact of cyberattacks.

How to cover the biggest cybersecurity risks to your organization

Threat #1: Phishing attacks

Phishing is one of the most common cyberattack vectors across all industries. According to the Health Sector Cybersecurity Coordination Center, 2021 brought a significant uptick in phishing attacks on the healthcare sector. In fact, throughout 2020, Akamai saw criminals leverage COVID-19 and the promise of financial assistance, or the stress of financial hardship, to target people across the globe via phishing.

Phishing attempts to acquire sensitive data through fraudulent emails or web pages. When successful, it compels a user to inadvertently enter their login credentials — essentially giving perpetrators an open door to the network.

This happened to those filing for unemployment in New York. According to a phishing report by Steve Ragan — former editor of CSO Online and current Akamai security researcher — there were several phishing kits targeting pandemic unemployment assistance (PUA) programs in early 2021. These are programs designed to assist those who needed help during the COVID-19 lockdowns, and provided essential services for millions of Americans.

In a spot on CBS News that aired across the country, Ragan discussed an unemployment phishing kit targeting people in New York and how criminals were collecting and selling personal information compromised in the scam. Since that news story aired, he discovered PUA scams targeting people in Wisconsin, Indiana, Pennsylvania, and Massachusetts.

How to stop and mitigate phishing attacks

Depending on permission settings and the security safeguards in place, gaining access to a single user account can potentially provide criminals with free reign to critical parts of your network, and they can often expand their reach once inside your organization's network.

Microsegmentation confines threat actors' access to only the portion of your network they initially gain access to, preventing them from moving laterally and leaving them unable to inflict further damage in additional areas. It limits the impact of a compromise by preventing criminals from using any entry point to access your broader organization's network.

In addition to microsegmentation, multi-factor authentication (MFA) is one of your best lines of defense against phishing attacks. It provides an added layer of protection by requiring additional identity verification before allowing access to an account, preventing compromised credentials from being exploited.

MFA, particularly a FIDO2-approved solution, ensures protection from the latest attacks and requires users to enter a unique code that's either generated through a text or authentication app on the user's mobile device. This additional login step helps thwart phishing attacks, even when criminals have accurate login credentials.

It's critical to educate your staff on the tactics of social engineering attacks like phishing. The reality is that phishing is one of those problems that doesn't have a silver-bullet fix, because there are so many moving parts. It's hard to predict what criminals will do next. Since humans are still a vital aspect in phishing, they will remain the weakest link in the chain.

This means that making security easy is essential. Akamai offers a frictionless, phish-proof MFA solution to protect against even the smartest cybercriminals.

Threat #2: Unsupported legacy software

Out-of-date software is another significant vulnerability concern. Each new security update (patch) that isn't immediately installed creates open backdoors on your network. This is especially true for older devices that age out of support and no longer receive updates.

Unsupported software can have zero-day vulnerabilities that organizations might be hesitant to patch on their own. Creating a custom patch can sometimes void a device's warranty, leading to costly repairs when something goes wrong.

While medical devices have a long lifecycle, if they aren't diligently updated with the latest version of the operating system, or are running an unsupported operating system, then hackers can exploit vulnerabilities to steal data, infiltrate a hospital network, and disrupt care. In fact, as many as 83% of internet-connected medical imaging devices — from mammography machines to MRI machines — are vulnerable, as reported by Fortune.

The older a device is, especially those beyond the maintenance lifecycle, the more likely criminals are to know the weak points that allow them to access your organization's network through a third-party device.

For example, Windows 95 has been out of maintenance for years, and yet many MRI machines (among others) still rely on that operating system since it was the last to enable direct writing. In-house developers might be able to patch a vulnerability, but their patch could void the warranty on the machine. The only safe option is to replace the MRI machine altogether, but that's cost-prohibitive for many facilities.

Network administrators try to keep unsupported systems off the network, but that's not always possible, especially when devices are needed for patient care and must quickly provide data to physicians. Isolation also fails when there is an incomplete map of all the devices connected to the network, creating backdoors. It's hard to protect what you can't see.

How to protect vulnerable, unsupported devices

To protect these devices from providing access to your organization's network, moving toward a Zero Trust Network Access (ZTNA) architecture is crucial. ZTNA is a framework that treats every incoming request as a potential threat until it is proven safe, effectively stopping attackers before they ever gain access to the device, even if your software is out of date.

Moving toward ZTNA marks a fundamental shift from the castle-and-moat approach of years past to a (verify-then-trust) Zero Trust model. While a Zero Trust approach likely won't protect against cyberattacks altogether, it limits the potential damage from catastrophic to manageable. HealthITSecurity says it best: "If a threat actor manages to get credentials and manipulate one device, it is unlikely that they will get much further with a Zero Trust architecture in place."

Akamai offers a robust plan to help providers move to a Zero Trust architecture, without the downtime and flexibility of current workflows. Get started on ZTNA with this blueprint guide.

Threat #3: Providers working from home and BYOD

Care continuity in the 21st century is decentralized. Patients receive care from the comfort of their homes. Providers give care via their mobile device rather than in person. But this increase in accessibility means that providers are seeing cybersecurity risks escalate dramatically as staff members oscillate between accessing networks on-site and from home, and log in from unmanaged devices.

While your team members may have occasionally logged in to your system from their home network prior to the pandemic, the increased volume of personal devices accessing your organization's network inevitably spiked during this period. If those laptops, tablets, or smartphones were infected with malware, they could become an entry point for a ransomware attack.

For example, if someone on your team falls victim to a phishing attack by accidentally entering their login credentials on a fake web page, malicious actors will have the same access the user has, potentially allowing them to encrypt files, lock out your team, and cripple your organization by demanding a hefty ransom to decrypt the files.

How to protect the edge of your network

By closely monitoring who is accessing your organization's network (where they are, what their IP address is, what device they are using, etc.), you can minimize the likelihood a situation like this will occur and work to stop an attack before it happens.

If your team uses personal devices or works from home, ask yourself these questions:

- Do we have a Zero Trust Network Access (ZTNA) approach in place to maximize scrutiny on incoming requests and stop an attack before it occurs?
- Have we established microsegmentation to limit access and prevent lateral movement if a criminal gains entry to the organization's network?
- Are we using a secure access service edge (SASE) framework to protect our network while minimizing latency and maintaining a fast and pleasant user experience?
- Is our team using access codes, strong and unique passwords, and multi-factor authentication (MFA) for each device and account login?

Akamai helps make network access management easy with our remote workforce security solutions.

Threat #4: Poor data flow mapping

With one foot on-premises and the other in the cloud, it can be nearly impossible to understand where your data lives and how it flows. This happens for a couple of different reasons.

First, volume. It can be overwhelming to keep up with the number of devices and applications being added and removed from your network on a daily — if not hourly — basis as vendors, contractors, and consultants all seem to use different devices, tools, and solutions.

Second, the system for tracking hardware and software has become defunct and is no longer accurate or reliable because of team member turnover, process changes, or competing priorities.

Regardless of the reason, it is important to visualize your network and connected devices, because you can't protect what you can't see.

How to map the flow of your connected devices

It's crucial to have a visibility tool that can create a roadmap of connected devices. Especially since a 2019 article in the HIPAA Journal cites that 82% of healthcare organizations had a cyberattack on their connected devices in the preceding 12 months.

Choosing a solution that tracks the flow of data across your network, telling you where it's coming from and where it's going — including devices that aren't connected to your network — is the first step in mapping your connected devices. This allows you to have a real-time network diagram of where information is flowing, and helps you discover devices with malicious intent that may be on your network. By putting software-defined microsegmentation rings around core systems, assets, and data (like PHI), your organization can limit the lateral movement attackers have within your network. Get the visibility you need with microsegmentation tools from Akamai.

Threat #5: Managing the complexity of networks, apps, and systems

Do you know which applications and software can read your data? Some software applications, like social media platforms, plainly state their invasiveness in their privacy statement or terms of service. Others, like email providers, are more covert but still pose a significant risk (e.g., having access to a device's photos when pictures contain PHI).

Apps might also be allowed to view items copied to the clipboard, including patient identifiers or passwords. If there is patient information on a device, there's a chance that a third party (or malicious actor) will see it (and record it).

Educate your team, view your entire network, protect your edge

It is crucial that you educate everyone at your provider organization on the risks of using personal devices and what is required to protect patients' private information.

It's also important to consider the view your organization has of your attack surface and potential vectors. Is your security team monitoring the entire network across multiple cloud service providers and on-premises data centers? Or are they siloed into various groups focused on different aspects of your organization's infrastructure? It's imperative to maintain a holistic view of your organization's entire network and its activity, especially during an attack.

Similar to threat #4, your best defense options for protecting the edge of your network are a Zero Trust architecture combined with microsegmentation and MFA for account logins. Employing one provider to protect all systems regardless of who they are owned by and whether they are in the cloud or on-premises will allow you to protect your network without hindering the user experience.

What is the impact of inaction?

Costs can take many forms. The most obvious is financial, with U.S. healthcare companies averaging $9.23 million in total costs associated with a single data breach, according to IBM's Cost of a Data Breach Report 2021. Other costs are more qualitative, like patient safety and trust, which can have an equal — if not greater — impact on healthcare organizations.

Reduced patient safety

Patient safety is the most significant target when it comes to cybersecurity. When IT systems are forced to shut down by an attack, patient care is disrupted. Treatments and appointments are postponed and can result in adverse health outcomes for patients. In fact, a recent lawsuit marked the first-ever allegation of a patient death resulting directly from a ransomware attack.

Meanwhile, connected medical devices used for remote patient monitoring (e.g., heart rate or glucose levels) pose a more direct threat to care. For instance, disrupting a patient's blood pressure readings might cause dangerous conditions to go unnoticed and untreated, potentially causing a sentinel event.

Loss of patient trust

The inability to provide reliable care and protect patient information leads to a loss of patient trust. More than 90% of patients say they'd switch providers if their private information was compromised in a data breach. The actual number might be lower when the time comes, but do the math: Even if only half of those patients left, or a tenth, what impact would it have on your patient population? And how long would you incur ongoing losses while gradually acquiring new patients?

Loss of revenue

At 38%, lost business is the largest cost factor associated with a data breach. When core provider systems go down (like EHRs, email servers, etc.), incoming business comes to a jarring halt. That means no appointments, no visits, no encounters, and no revenue (not to mention the impact it has on patient care).

San Diego–based Scripps Health suffered a major cyberattack in May 2020 that resulted in $91.6 million in lost revenue, primarily from reducing the volume of emergency department care and elective surgeries.

Even if some parts of the health system's network are still operational, you can't be sure everything is safe until you've located the vector, patched the vulnerability, and completed the forensics analysis.

Increased overhead

Recruiting, hiring, and retaining coveted cybersecurity engineers is expensive, but the true costs go far beyond that. Employing a homegrown cybersecurity team at your organization can leave you with expensive gaps in coverage.

Generally speaking, the longer it takes for your organization to identify and exfiltrate a threat actor from your network, the higher the costs will be. A report from Ponemon Institute states that detecting a cyberattack within the first 200 days can save an organization more than $1.26 million. Unfortunately, according to the same report, the average attack takes 287 days to identify and contain. *287 days!* That means threat actors are often inside the network infrastructure for more than nine months, plotting and planning their attack to inflict maximum damage to your hospital's reputation and bottom line.

It is essential to quantify the amount of time your security team requires to identify and take action against an attack. Consolidating security vendors to those who offer managed services and engineering support for staff surges can present significant cost savings.

Regulatory fines

With so much valuable personal information in your charge, a data breach could lead to heavy fines from regulatory agencies. As of November 30, 2021, the Health and Human Services Department's Office of Civil Rights has settled or imposed penalties against 106 HIPAA-covered entities for a total of more than $131 million. That's an average of over $1.2 million per penalty (on top of the additional costs mentioned here).

How to best prepare your healthcare organization for a cyberattack

Today's cyberthreats require provider organizations to have industry-leading security. Your patients and your business depend on it — the cost of inaction is too high.

Financial constraints, competing priorities, or uncertainty of the risks might push you toward taking on too much risk. But your security efforts must be thorough, strategic, vigilant, and agile.

An adequately protected ecosystem today is not necessarily protected tomorrow. Threats evolve quickly. A day (or less) can be all it takes for threat actors to exploit a new vulnerability.

Providers looking to reduce that threat area and take the advice of the backup approach outlined in the federal advisory — saving three copies in at least two different formats, with one offline — are increasingly looking for a hybrid approach. On-premises data storage provides them with more control over security, but it can be costly and difficult to expand at the pace needed, especially with the current explosion of health data and the digital transformation in care, both spurred by the pandemic. Public cloud data storage is more cost-effective, but organizations risk outages and a lack of transparency into how the data is protected.

A hybrid approach allows sensitive data to be kept on premises, while less sensitive data is stored in the cloud. Even this is not perfect, as security must be put in place to protect the transfer of data between the two storage types and ensure that access is limited to those who are authorized to make the transfers and view the data. Moving toward the seven key requirements for implementing a ZTNA architecture helps enable institutions to protect their data, by granting users access to only those applications they need for their role, with further security offered by MFA.

Akamai is here to help you prepare for when — not if — an attack occurs. Let's work together to build a cohesive view of your network to quickly spot an attack and efficiently mitigate the damage. Our business is built on protecting networks from distributed denial-of-service and ransomware attacks to deliver seamless, secure web experiences (including apps and APIs).

We fortify the edge of your network to limit your chances of a breach, as well as reduce the blast radius when one occurs. And we do it while retaining flexibility for user access, so your organization can focus on providing optimal health outcomes amid ever-changing operational and care demands.

Protecting your patients' information from the increasing sophistication of cybercriminals and an expanding cloud-based attack surface has never been more important. Patient-centric organizations and government entities trust Akamai's edge platform to keep their digital experiences closer to patients — and threats farther away.

Trust Akamai, the partner that will turn cybersecurity from a perpetual burden to a competitive strength.

Contact us to learn more, or give us a ring at +1-877-425-2624.

Akamai powers and protects life online. The most innovative companies worldwide choose Akamai to secure and deliver their digital experiences — helping billions of people live, work, and play every day. With the world's largest and most trusted edge platform, Akamai keeps apps, code, and experiences closer to users — and threats farther away. Learn more about Akamai's security, content delivery, and edge compute products and services at www.akamai.com and blogs.akamai.com, or follow Akamai Technologies on Twitter and LinkedIn. Published 02/22.