BIZCOMMUNITY

Healthcare is now the industry most targeted by hackers

By Byron Horn-Botha

18 Jul 2022

Global reports indicate that healthcare data breaches reached a record high in 2021. Indeed, healthcare now sees more cyberattacks than any other industry.

Byron Horn-Botha, business unit head at Arcserve Southern Africa.

Fully one-third of all cyberattacks are aimed at healthcare institutions. Why? Because healthcare is a valuable and vulnerable target.

South Africa is no stranger to this trend, with pharmacy giant, Dischem, hitting the headlines in May this year with a breach that resulted in over 3.6 million records exposed following the attack.

Hackers go after healthcare because patient data and hospital systems are lucrative prey. Hackers know they can demand a high ransom if they compromise patient data or healthcare systems.

They also know healthcare organisations will likely pay the ransom — and fast because compromised data and systems can cost lives in a hospital setting.

Hospitals, of course, rely on constant and immediate access to patient data to deliver care. If they don’t have that access, people may become even more ill and die. Almost one-fourth of healthcare institutions hit by a ransomware attack in 2019 and 2020 reported increased patient death rates after the attack.

Unfortunately, attacks on healthcare will only increase in the years ahead. Indeed, some hacking groups focus solely on attacking healthcare organisations. In April of this year, the US Department of Health and Human Services warned the healthcare industry about “an exceptionally aggressive” ransomware gang called Hive dedicated to targeting healthcare and favours double extortion.

It demands one payment to unlock data it has encrypted and another payment to prevent the data from being publicly released.

Air gapping can protect healthcare data

Ransomware works by traversing all copies of data, including primary, secondary, and backup data. Attackers then encrypt or exfiltrate the data. Air gapping is one of the most practical and effective ways to secure backup data against a ransomware attack.

There are two types of air gapping. The first is traditional, physical air gapping, in which an organisation disconnects the digital asset from all other devices and networks. This air gapping is the ultimate cybersecurity measure because it creates a physical separation between a secure network and any other computer or network.

Using a physical air gap, organisations store backup data on media such as tape or disk, then disconnect these media entirely from their production IT environment.

Kenyan healthtech launches universal patient portal

11 Jul 2022

The second type of air gapping is called logical air gapping. A logical air gap relies on network and user-access controls to isolate backup data from the production IT environment. It’s like a one-way street on which data is pushed to its intended destination, whether that be a storage device on-premises or a custom appliance.

The key here is that the control and management of that data, such as how it is retained or who can modify it, is unavailable through that same system or path. Anyone who wants to manage or alter the data must use entirely different authentication channels.

The beauty of air gapping is that it makes it nearly impossible for ransomware to compromise your data backups. It’s almost as if your data is wearing a cloak of invisibility, making it impervious to any malware that manages to enter your network.

Another vital step is 3-2-1-1 data protection

Healthcare organisations can deploy a second measure against ransomware, 3-2-1-1 data protection. It means maintaining three backup copies of your data on two different media, such as tape and disk, with one of the copies placed offsite to enable quick recovery.

Further, you should have one immutable object storage copy of your data and one air-gapped copy. Immutable object storage continuously protects data by taking a snapshot at 90-second intervals. So even if a ransomware attack occurs, you can recover your data immediately.

If there is an attack—or downtime or natural disaster—your data snapshots enable you to return to a current file state.

Snapshots can’t be changed, deleted, or overwritten, so they secure data against ransomware attacks, human error, and hardware failure.

Healthcare organisations that deploy immutable snapshots can continue their operations seamlessly even in a ransomware attack or other calamity.

Hospitals must move fast to secure their data

For years, companies could rely on a cyber strategy of safety in numbers, figuring that the bad guys would attack someone else. That strategy is now out the window. Healthcare organisations must assume that they will, sooner or later, be the target of a ransomware attack.

The impact of a data breach in healthcare can be catastrophic since all aspects of healthcare are now digital, from diagnosis to long-term care to every event in between.

Healthcare generates vast volumes of data at all levels of care and engagement—and that data could not be more critical because human lives depend on it.

Given the quantity and value of healthcare data, implementing a multi-layered protection and recovery strategy is urgent.

ABOUT THE AUTHOR

Byron Horn-Botha is the business unit head at Arcserve Southern Africa.