DARKReading

10/26/2018
10:30 AM

Joe Merces
Commentary
Connect Directly

3 Keys to Reducing the Threat of Ransomware

Following these steps could mean the difference between an inconvenience and a multimillion-dollar IT system rebuild -- for the public and private sectors alike.

When I was a CIO in New York City government, we used to say there are two types of organizations: those that have been compromised and know it, and those that have been compromised and don't know it. That (and the anxiety of whether data is being stolen or changed) keeps CIOs awake at night.

As recent ransomware attacks are making news globally for their mounting costs, it's obvious that once they've been hacked, these organizations discover there are deeper problems in their infrastructure or security hygiene that ransomware has exploited.

You've probably read about the city of Atlanta, which was infected by the SamSam ransomware, and the $17 million headache it caused. The city opted to rebuild its entire IT infrastructure, which accounted for most of that cost.

But Georgia is not alone.

This spring, the Erie County Medical Center in Buffalo, N.Y., was infected and blackmailed to release private keys held for ransom. ECMC opted to rebuild its infrastructure rather than pay a ransom; the cost has rocketed to $10 million.

At the same time, the Colorado Department of Transportation was hit twice by the same ransomware, when a SamSam variant reinfected its cleaned system. It has decided to rebuild all of its IT systems, at a cost approaching $2 million.

These are real head-scratchers. You'd think that spending taxpayer dollars to rebuild everything from A to Z would be a last resort. Wouldn't it be more sensible to pay for a third-party review of security hygiene and posture, and bolster it wherever it's lacking, including penetration testing?

Why rebuild? Maybe there was something wrong in the IT architecture, or the systems were outdated and needed replacement. Maybe the fear of something being left behind that might cause reinfection was too much to bear. We may never get the full story, but we do know the enormous cost of rebuilding these systems.

As a CIO, I experienced numerous attempted ransomware attacks and several instances of server encryption, or attempted encryption, where we were able to take servers out of rotation. Fortunately, ransomware then was not what it is now, and though we were attacked our backups were not affected.

Luck wasn't the only reason we were able to recover so quickly. We used good cyber hygiene and best practices to reduce the hacking threat. We also took snapshots of our infrastructure every 30 minutes, with full backups nightly. We always recovered with minimal data loss.

Avoiding ransomware problems boils down to three basic approaches that apply in general to both private and public sector organizations: good cyber hygiene and user training, best practices, and routine testing of backup and recovery plans.

Cyber Hygiene and User Training

Starting at the obvious, good cyber hygiene must require regular password changes, with passwords of certain lengths, and special characters.

Have passwords for everything. Remote Desktop Protocol (RDP) accounts are sometimes overlooked, but public-facing servers *must* have passwords to avoid exposing information to prying eyes. Passwords for RDP accounts should be complex and not something simple as "password123," which hackers will try in brute force attacks.

Phishing is still commonplace. You'd be surprised how much spam floods into private and public sector organizations. You'd also be surprised by how many people still click on infected emails, PDF images, and documents.

Routine user training is essential for users to understand the ramifications of clicking without thinking.

Best Practices

Best practices start at the desktop, by continuously pushing patches and updates. Keep up with updates or you'll risk infection from problems across multiple desktops and connected server resources.

Regularly push out operating system patches, zero-day vulnerability patches, and security updates. Be tenacious in keeping operating systems up to date. If you're sitting on an unpatched vulnerability, you risk having it used against you.

You also need preventive security technology to survive in today's world. Cloud web application firewalls must be used and appropriately set, and ports blocked. Otherwise, you *will* be hacked.

Good communication is essential. The IT experts putting together your servers may not also be security experts. They need to be very tightly coupled with your security information officer and his team — and the team responsible for backup.

Testing Disaster Recoverability Plans

Most organizations do not actively test whether their backup and disaster recovery plans actually work. They are just making backups, and when they restore, they may be going backward into backups that don't actually work or may not bounce back from advanced persistent threats.

The cloud makes it simple to back up, take snapshots and replicate objects to other regions and accounts, adding layers of disaster recoverability that can benefit any enterprise when recovering from a cyber disaster.

These simple steps may not completely protect you from ransomware, but in my experience, they're the difference between an inconvenience and a multimillion-dollar IT system rebuild.

Related Content:

- 7 Key Stats that Size Up the Cybercrime Deluge
- Ransomware Attack Hits Port of San Diego
- NC Water Utility Fights Post-Hurricane Ransomware
- Cybercrime-as-a-Service: No End in Sight

Joe Merces is a talented and seasoned executive with more 30 years of extensive experience in cloud services, information technology, cybersecurity, and data communications, with a diverse background in both private and public sector settings. Prior to founding Cloud Daddy in ... View Full Bio

COMMENT | EMAIL THIS | PRINT | RSS