Technically Speaking

Do You Have a Cybersecurity Playbook?

By Bryce Austin

I have been investigating a large number of failed logins on your server. Due to the volume of failed attempts, it does appear the attempts are coming from an outside source. My company recommends you reach out to a security firm to have your network investigated for a possible breach.

He couldn’t believe what he was reading.

A local cybersecurity professional was forwarded the email above from his new client’s outsourced computer management company. The owner of the business was concerned, and for good reason.

They had only brought him on board as a part-time cybersecurity advisor the month before, and the vendor that manages the network had kicked this ball squarely into his court. He had to figure out what to do – fast.

The priorities were simple:

- Alert his client’s executive team about the situation.
- Determine if this was or was not a real hacking attempt.
- If it was a real hacking attempt, determine how it was occurring.
- Assess if the hack was successful in any way. Was any damage done? Was any data accessed?
- If the hack was unsuccessful, terminate the hacker’s access immediately.
- If the hack was successful, start making calls to his client’s CEO and cybersecurity insurance carrier, a third-party company that specializes in breach remediation and his client’s attorney.
- Follow up with root-cause analysis and recommend preventive measures.

It took more than 10 hours to determine the extent of the issue. Cybercriminals had breached a single server and a malicious program was running on that server.

It was trying various dictionary words as passwords against common “administrator” level accounts. He breathed a tiny sigh of relief to see it had only started several hours earlier and appeared to be moving ahead at full steam, which meant the bad guys had most likely *not* yet been successful at cracking an administrator-level password.

The cybercriminals gained access to that server via a combination of a phishing email and a bad firewall configuration. Thankfully, forensics found no evidence of further intrusion.

His blood pressure began to return to a more reasonable level.

The example above is real, and while it represents the best possible outcome of a cybersecurity incident, it was used here to make a number of points.

That client didn’t have a playbook on what to do when a cybersecurity incident is suspected, so those involved had to make it up as they went. Doing so took extra time and might have led them to miss obvious steps.

The company did not have documents outlining how to bring operations back online if the hack had been successful, nor did it have procedures to follow if it was determined any sensitive data had been stolen.

Its IT services vendor wasn’t well trained in how to get to the bottom of the technical issues quickly, which lengthened the incident by hours.

The client didn’t have a list of whom to call if a cybersecurity incident was suspected, which made the phone number to its cybersecurity advisor the only number anyone thought to use. What if he was unavailable when this took place?

In a nutshell, the client didn’t have its act together, and it showed.

After an incident occurs, your company will be judged on the following criteria:

- Before the incident, did your company take all actions one would expect of a prudent organization to prevent the incident?
- Did your company respond to the incident using procedures one would expect of a prudent organization?
- Are there any ways the media could portray your actions to make your company appear to be culpable or incompetent? If so, expect that they will.

A robust playbook that includes the CEO, chief legal counsel and all other senior leaders will do immeasurable good in your ability to respond to an incident.

An incident response playbook needs several key elements to be effective. It must:

- Identify who in your organization has the authority to declare a cybersecurity incident. Who can initiate the playbook?
- Spell out how much money that person can authorize to have spent to have an incident investigated or remediated.
- Have a list of the types of scenarios the playbook is designed to cover. Examples include the loss of sensitive data, a ransomware attack, the loss of a critical system, natural disasters, law enforcement contacting your organization about a warrant or subpoena and the loss of the use of one or more of your sites due to a natural disaster or because of other issues (such as a crime taking place in the building and the police barring your employees from entering the premises).
- Have a call tree that includes which people or groups to call when an incident takes place.
- Define the people or groups responsible for making the decision on when to bring in law enforcement.
- List the people authorized to speak to the media about a cybersecurity incident and what those who are not authorized to speak to the media should say if they are approached by a reporter.

- List all of your critical systems, the location of the data in those critical systems and the location of the backups for the data for those systems.
- Outline your general incident response process. While every scenario is different, the process normally follows certain steps: preparation, detection/analysis, containment, eradication, recovery, incident closure/root-cause analysis and preventative measures.
- Be reviewed on a frequent basis. Plans get stale quickly and need to be reviewed whenever a significant change in your organization takes place.

If the above points are reviewed as a group, an interesting trend emerges: most of them are non-technical.

The majority of them are operational and financial in nature.

That is a critical misstep in many incident response plans. If your technology team manages your incident response plan, it is making business and financial decisions that should be made by CEOs, COOs, CFOs and legal counsel.

Above all, your incident response plan needs to be tested. Unless you have rehearsed an incident response procedure, you're only able to guess if it will work.

Cybersecurity is too important to be left to guesswork.

So what are the takeaways?

- Your company needs an incident response playbook.
- The incident response playbook should be owned by a non-technical member of your executive team.
- Your company needs to periodically test your incident response capabilities.
- Your company needs to update the playbook from lessons learned as a result of tests, whenever significant changes occur to the operational or technical aspects of the company or when merger/acquisition activity occurs.

Bryce Austin is CEO of TCE Strategy, a speaker on emerging technology and cybersecurity issues and author of Secure Enough? 20 Questions on Cybersecurity for Business Owners and Executives*. With more than a decade of experience as a chief information officer and chief information security officer, he advises companies on effective methods to mitigate cyber threats. For more information, visit www.bryceaustin.com.*