09
MAY

5 Things an Enterprise Must Do if There's A Security Breach

May 9, 2016 / Ryan Nolette / Advanced Threat Protection, Community Perspectives, Detection and Response, Endpoint and Server Security, Prevention

No one is immune to security breaches. Targets will vary in value and cause, but there is no such thing as

an "off limits" organization to a motivated attacker. Building out a united, defense-in-depth security posture will help you more than any single product available.

User training and active defenses (drills, pen tests, vulnerability scans, etc.) are worth their weight in gold. By being active and chaining your security stack – from the perimeter to the endpoint and back – you are reducing your risk surface.

Remember: reducing risk is a process, not a destination. That process will have to be repeated over and over again to stay current, to scale and to be effective.

Following the "be active" approach above will limit how often you have to perform a response engagement, but what do you do once you have a breach?

Below are my top five things to do once a breach is discovered:

1 – Take a deep breath

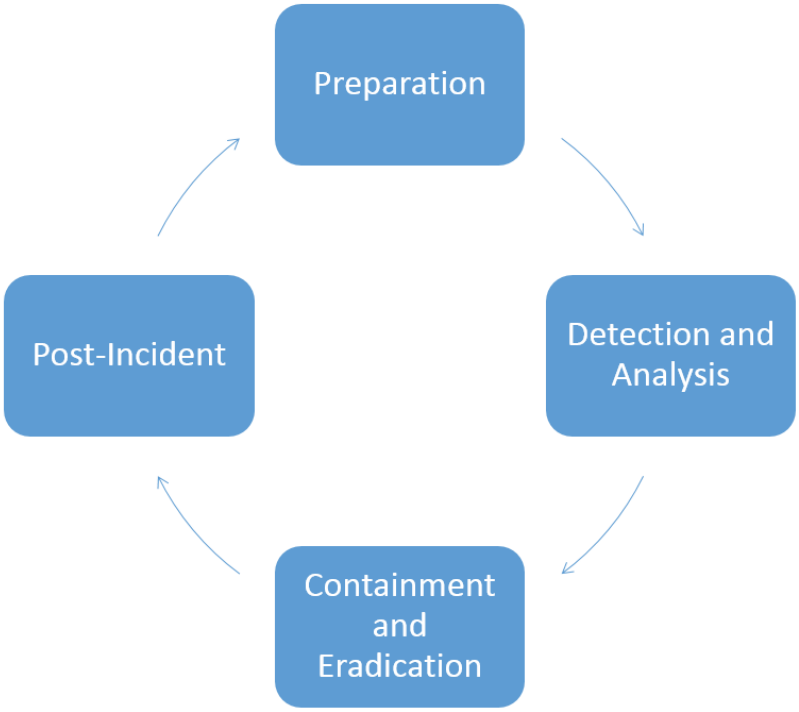
Panic and anger will help no one in this situation. It is important to take the extra minute to think about your next steps.

2 – Get out your breach playbook and build your war room

You have one of these playbooks, right? Or did you expect to never be breached? You never expect to crash your car either, but you still pay for insurance and wear your seat belt, just in case.

3 – Execute your playbook

The "Security and Privacy Incident Response Process" is a well-defined and organized four-step approach to handle security and privacy-related incidents. This process is my current go to for process and workflow during an IR.



Preparation: Define the process, classification methodology, escalation path, necessary resources, roles and responsibilities. Assign ownership.

Detect and analyze: Use defined monitoring and reporting channels to detect security events and determine their assessment and routing.

Containment, Observation (if appropriate), Eradication, & Recovery: Begin damage-control activities and determine the containment strategy. Return systems to normal business operations and, to the extent necessary, notify the relevant internal and external parties regarding the incident.

Post-Incident Activity: Learn lessons from the incident and create a remediation plan in an effort to reduce the probability and impact of similar incidents in the future.

4 – Responsible disclosure

Responsible disclosure is a tech term describing a vulnerability disclosure model. Often used interchangeably with terms such as "full disclosure," responsible disclosure has the additional caveat that all stakeholders agree to allow a period of time for the vulnerability to be patched before publishing the details. I use this model, slightly modified of course, to determine what level of disclosure is required by local and federal law, company policy, and user agreements. Remember, we live in a world where secrets do not remain secret for long. A disclosure announcement coming from you will not damage your reputation more than details of the breach getting leaked online.

5 – Learn from your mistakes, identify your gaps, and implement projects to repair broken processes and blind spots, assess your new risk surface, rinse and repeat.

This is the stage where the active approach cycle I noted above becomes very important. Identifying the factors that led to the breach will reveal the gaps in your armor and shed light on new gaps that attackers did not exploit in the previous breach.

No one is immune to security breaches. By being active and building out a united, defense-in-depth security posture with policy, user training, and new technological controls will help you reduce your risk surface.

Remember: Reducing risk is a process, not a destination. It will have to be repeated over and over again to stay current, to scale, and to be effective.

Until next time, remember my motto: "Flag it, Tag it, and Bag it."

Ryan Nolette, is the Security Operations Lead at Carbon Black and draws from more than decade of intense and active Incident Response (IR), Threat Research, and IT experience to add a unique perspective of technical expertise and strategic vision to Carbon Black. Prior to running SecOps, Ryan was a Senior Threat Researcher and Senior Incident Response Consultant for Carbon Black and previous companies.

https://www.linkedin.com/in/ryannolette

https://www.carbonblack.com/author/ryan-nolette/

Tags: Carbon Black | incident response | Ryan Nolette

More Posts