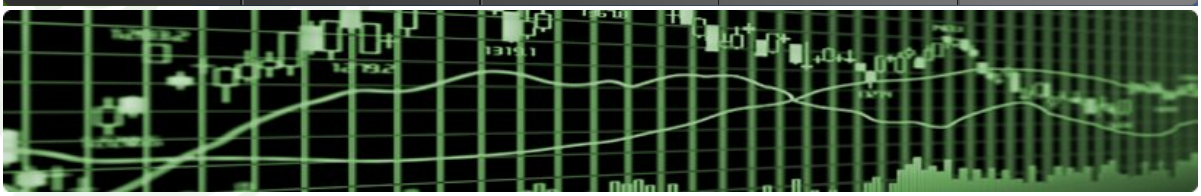

NEWSLETTER
Feature Stories
Cyber Tips

ACSC NEWS

CYBERSECURITY NEWS
2015
2014
2013
2012
2011

EVENTS
2015
2014
2013
2012
2011

Cyber tips: 5 things to do when a breach occurs

May 5, 2016
By Ryan Nolette

No one is immune to security breaches. Targets will vary in value and cause, but there is no such thing as “off limits” to a motivated attacker. Building out a united defense in depth security posture both by policy as well as by technological controls will help you more than any single product offering regardless of what their sales team is promising you. User training and proactive defenses (drills, pen tests, vulnerability scans, etc) are worth their weight in shiny new products with unlimited marketing budgets. By being proactive and chaining your security stack, from the perimeter to the endpoint and back, you are reducing your risk surface. Remember that reducing risk is a process, not a destination and will have to be repeated over and over again to stay current, to scale, and to be effective.

Following the “be proactive” approach above will limit how often you have to perform an IR, but what do you do once you have a breach? Below are my top 5 things to do once a breach is discovered:

1. Take a deep breath. Panic and anger will help no one in this situation. You should also 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 never to be breached? You never expect to crash your car either, but you still pay for insurance and wear your seatbelt, 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 four-part 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. Then assign ownership.
- **Detect and analyze**: Use defined monitoring and reporting channels to detect security events and determine their assessment and routing.
- **Containment, Observation, 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**: Take steps to 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. Provide responsible disclosure. Responsible disclosure is a technology term describing a vulnerability disclosure model. Often used interchangeably with terms like 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. 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, implement projects to repair broken processes and blind spots, assess your new risk surface, then rinse and repeat. This is the stage where the proactive approach cycle I spoke about above really becomes important. Identifying the factors that led to the breach will tell you where the gaps in your armor are and will shed light on new gaps that the attackers did not exploit in the previous breach.

In closing, no one is immune to security breaches. But when you're proactive in building out an in-depth security posture with policy, user training, and new technological controls, you will significantly reduce your risk surface. Remember that reducing risk is a process, not a destination and will have to be repeated over and over again to stay currently, 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. Read more at his blog: https://www.carbonblack.com/author/ryan-nolette/