KIVU

Peeling Back the Layers on Incident Root Causes

Across the thousands of incidents that Kivu has investigated since its founding in 2009, the overwhelming majority can be traced to one of two events - exploitation of a previously known but unpatched software vulnerability or a successful phishing attack (i.e., an unwitting user clicked a link or opened an attachment that they shouldn't have). These "root causes" are where investigators usually can first identify evidence of the compromise. Victims and insurance carriers can accept these as the root causes because they are easy to define in terms of a time and a location in the environment where they occurred. In short, they're simple and clear cut.

However, the real story of an incident is usually more abstract and more complex. In many cases, root causes identified by incident investigators are just symptoms of deeper security issues. Getting to the root of a root cause and devising a corresponding remediation plan requires more analysis.

Examining A Complex Chain of Events

When determining how an incident occurred, defenders should approach their analysis similar to how accident investigators examine plane crashes. Consider the notional example of a pilot who crashes while flying in poor weather. The pilot might describe the accident's root cause as something unexpected and unavoidable that immediately preceded the crash. "I was flying along when an afternoon storm blew in. I decided to turn back, but the weather worsened. Finally, when attempting a landing at my home airport in heavy rain, a strong downburst slammed the plane into the ground just short of the runway."

To the pilot, the root cause of the accident would likely be the downburst. This weather phenomenon often accompanies thunderstorms and generates winds with a downward force that can easily throw small planes to the ground. It can't be predicted or avoided, making it especially dangerous. Although the downburst is an immediate cause of the plane crash, a chain of events preceded that phenomenon starting when the pilot decided to make the flight.

In this example, accident investigators will ask questions about the condition of the aircraft, the pilot's knowledge and experience, and pre-flight planning. Ultimately, investigators might uncover a deeper root cause of the incident after learning that the pilot simply didn't check the weather before flying. Investigators may conclude that the accident resulted from the pilot's lack of training or because he was careless.

Determining the ultimate "root cause" is vital because if the client was inexperienced or accident-prone, he or she will be required to take additional training to close identified knowledge gaps. Without that training, chances are higher that another accident will occur in the future.

The Five Whys

When compared with the air accident investigation, a cybersecurity investigation requires even greater emphasis on identifying underlying conditions and understanding the chain of events. Victim organizations shouldn't simply rely on the investigator's findings of the direct cause, but instead should use those findings to perform their own analysis of the true root cause.

A simple approach to uncovering a true root cause of an incident is the "five why's" analysis. Victims should try to construct a chain of events by asking "why" for each step. What condition preceded the last known failure? Then, repeat the question enough times (maybe five, maybe more or less), and the victim develops insight into underlying conditions that enabled the chain of events to occur.

Examining A Complex Chain of Events

Let's try it with a notional cyber-attack. Using the "five why's" analysis, a typical ransomware incident with an unpatched software vulnerability initially identified as its root cause, might go this way:

Root Cause Analysis

Attackers exploited a publicly known web server vulnerability that went unpatched.

Why 1 — Why was the vulnerability unpatched?

The victim never realized the vulnerability was present on its web server.

Why 2 — Why did the victim fail to discover the vulnerability?

The victim failed to regularly scan or penetration test for security vulnerabilities.

Why 3 — Why didn't the organization work to identify vulnerabilities on a regular basis?

The organization has not established a vulnerability management program that includes capabilities for vulnerability identification and remediation on an ongoing basis.

Why 4 — Why doesn't the organization have a vulnerability management program?

No one on the victim's team has any cybersecurity training or experience, and they were not aware of the needed capability.

It's helpful to stop when the analysis reaches threshold issues that the victim organizations could reasonably control. Continuing the analysis likely would create increasingly abstract insights with no actionable outcomes (e.g., the organization lacks a culture of risk management, no budget, etc.).

KIVU

Addressing Actual Root Causes

Identifying an incident's true incident root cause helps to prevent a repeat of the incident. However, too many organizations become distracted by symptoms of underlying conditions rather than addressing actual root causes themselves. While patching an already exploited vulnerability serves an immediate need, it does not build a culture of security.

Security service providers can deliver significant value for low cost by delivering a thoughtful "five why's" analysis to identify true incidents. In addition, managed security service providers can help to affordably address the outcome of the analysis. For example, an effective solution for our notional incident might be to conduct vulnerability scanning on a quarterly basis while also updating an existing IT service provider contract to include responsibility for patching identified vulnerabilities based on the outcomes of scans. Vulnerability identification via endpoint protection agents on servers and workstations might also be added to further improve the team's ability to identify vulnerabilities over scanning alone.

Going Beyond Insurance

Cyber insurance mitigates significant risks for businesses by providing them with a mechanism to control losses when incidents occur. It also provides key expertise and support when an incident occurs. Insurers connect victims to service providers who provide the immediately needed triage. Unfortunately, organizations sometimes mistake the services covered by the insurance carrier with the effort needed to mitigate cyber risk appropriately. By performing additional analysis on the identified root causes of security incidents, victims will discover the issues that need remediation and can take appropriate action to ensure that they've addressed real root causes and not just the symptoms.

Contact us to learn more at
info@kivuconsulting.com

Kivu is a leading global cybersecurity firm dedicated to offering best-in-class cybersecurity services. Since 2009, Kivu has been providing a full suite of services covering the entire incident lifecycle, specializing in the forensic response to cyberattacks and ransomware incidents.

If you are experiencing a suspected active data incident, contact us at
incidentresponse@kivuconsulting.com or call
+1 855.548.8767 (United States) or **+44 203.997.8334 (Europe).**

KIVU