PLANNING FOR FAILURE

WHY IT IS IMPORTANT TO HAVE AN INCIDENT RESPONSE PLAN IN PLACE BEFORE YOUR COMPANY IS BREACHED

To explain simply, cyber incident response (IR) means a methodology of what should organisations do in the event of a security breach to limit damage and reduce recovery times. Dealing with the aftermath of a security incident often requires the efforts of the entire organisation. A well- crafted IR plan entails which key executives should be notified when a breach occurs and how this information needs to be communicated both within the organisation and externally.

Ryan Trost

"Cyber incident response is a critical discipline within security operations in order to reduce the adversary dwell time within an environment. Primarily to ensure the successful remediation of malicious attacks, but also, to help determine the necessary countermeasures to mitigate future attacks. IR is the ability to identify and track an adversary's movements through a network by utilising various analytical measures to discover the initial attack vector, patient-0, lateral movement and uncover the adversary's motives and objectives,"

Meet us @ **GITEX2019**
Finesse Booth No. 09, Hall No. 07

Enabling Digital Transformation

- *AI & CHATBOTS*
- *BLOCKCHAIN*
- *CUSTOMER EXPERIENCE MANAGEMENT*
- *BI & ANALYTICS*
- *ROBOTIC PROCESS AUTOMATION*

FINESSE

MENA | APAC | AMERICAS

No.1 Trusted Software System Integrator..!

350+ Professional Team | 250+ Enterprise Clients | 40+ International Awards
10+ Global Locations | 20+ Nationalities

finessedirect.com | finessedirect | +9714 3300144 | info@finessedirect.com

Manikandan Thangaraj

says Ryan Trost, co-founder and CTO, ThreatQuotient.

By studying the adversary and their tactics, techniques, and protocols (TTP) the IR team can make the necessary defensive adjustments to strengthen the organization and to avoid repeating past security lapses. Without a cyber incident response team, an organisation is doomed to constantly repeat previous failures in defending their environment against malicious adversaries, he says.

The first step in creating a solid cybersecurity strategy is to assume the worst-case scenario, such as the organisation facing a cyberattack, according to Manikandan Thangaraj, vice president at ManageEngine. "A good security strategy not only looks at ways to proactively detect and prevent attacks; it also documents how the business should react following an attack. An incident response (IR) plan is an important part of any IT security strategy. "

A recent study from IBM exploring organisations' preparedness in Saudi Arabia and the UAE when it comes to withstanding and recovering from a cyberattacks revealed that approximately third of organisations are still unprepared to respond to cybersecurity incidents, with 31% of respondents indicating they do not have a cybersecurity incident response plan in place.

While studies show that companies who can respond quickly and efficiently to contain a cyberattack within 30 days save over $1 million on the total cost of a data breach on average, shortfalls in proper cybersecurity incident response planning have remained consistent over the past four years of the IBM study. Of the organisations that do have a plan in place, almost half (49%) do not test their plans regularly, leaving them less prepared to effectively manage the complex processes and coordination that must take place in the wake of an attack.

For organisations with IR plans, it is also equally important to review the security checklist often. "Incident response plans can be highly complex as many get as granular as to define a standard operating procedure (SOP) with parallel workflows. Periodic reviews of incident response plans are important to ensure everybody is familiar with the process, not only on the incident response team but also within the larger security department. These planned IR reviews can range from simply updating contact information, and elaborate tabletop exercises to "after-action" debrief efforts to review lessons learned based on the results of the attack. Incident response procedures are even more paramount when the security operations team spans multiple shifts, geographic locations, access control or role responsibilities," says Trost from ThreatQuotient.

> "CYBER INCIDENT RESPONSE IS A CRITICAL DISCIPLINE WITHIN SECURITY OPERATIONS IN ORDER TO REDUCE THE ADVERSARY DWELL TIME WITHIN AN ENVIRONMENT. PRIMARILY TO ENSURE THE SUCCESSFUL REMEDIATION OF MALICIOUS ATTACKS, BUT ALSO, TO HELP DETERMINE THE NECESSARY COUNTERMEASURES TO MITIGATE FUTURE ATTACKS. IR IS THE ABILITY TO IDENTIFY AND TRACK AN ADVERSARY'S MOVEMENTS THROUGH A NETWORK BY UTILISING VARIOUS ANALYTICAL MEASURES TO DISCOVER THE INITIAL ATTACK VECTOR, PATIENT-0, LATERAL MOVEMENT AND UNCOVER THE ADVERSARY'S MOTIVES AND OBJECTIVES."

Thangaraj from ManageEngine agrees with this view. "Creating an incident response plan should not be treated as simply checking an item off a to-do list. Many organisations prepare an IR plan, and then put it away on a shelf. Instead, risk-averse organisations should review their plan regularly, as well as whenever an incident takes place.

"Business-critical asset and application inventories change all the time. An IR plan should look at how to restore these assets as quickly as possible. It's also critical to reflect after each incident and incorporate any findings into the IR plan. The goal should always be to decrease the MTTC."

Should enterprises automate incident response? The answer to this question depends on who you ask.

Yes and no, says Trost from ThreatQuotient. The ability to automate incident response efforts from start to finish is a mythical utopia the industry never truly reach because most incidents are never that black and white. Motivated adversaries are too crafty and disciplined for the industry to rely completely on IR automation. "From several of my past experiences against highly motivated, nation-state adversaries, I have learned that an IR team must think outside the box in order to successfully reclaim the network; which is impossible to automate fully. There is room for automation within incident response, but it resides in the earlier steps of incident response that focus on "IR smoke screen tests" as well as, information gathering/ collection efforts including pulling any pertinent application or network logs or querying threat intelligence repositories, he adds.