THE CONNECTWISE INCIDENT RESPONSE GUIDE

THE CONNECTWISE INCIDENT RESPONSE GUIDE

A new survey of 2,400 IT and security professionals conducted by The Ponemon Institute on behalf of IBM finds 66 percent of respondents say their organization is not prepared to recover from cyberattacks. A growing trend is to let MSPs handle cyberattacks and other critical incidents. Those with experience have an incident response plan in place to cope with any disruption to their business. [1]

AS AN MSP, DO YOU HAVE AN INCIDENT RESPONSE PLAN IN PLACE?

The goal of this white paper is to bring forth some ideas on perfecting your incident response plan through ConnectWise and critical alerting.

PRE INCIDENT PREP WORK

SETTING UP ALERTS

The beginning of an incident is perhaps the point where you have the most control. Most systems that are under your care will send off an alarm if something is not right. Most of these notifications are in the form of email. Emails however are not effective as most inboxes burry important alert. Email tends to be easily ignored because they don't come with a blaring audible alarm that draws your attention. Any system that sends off an email notification should be integrated with a monitoring tool or an alerting app that can be accessed using any smartphone, anywhere.

BE SMART – USE A SMARTPHONE

Smartphones are a miracle to those who work with random things that go bump in the night. The alternative is the antiquated pager. Pagers are unable to continue alerting until the messages are read. Smartphones on the other hand are readily available. Let's face it, who today doesn't have a smartphone? Furthermore they can host apps that act like pagers.

While there are a lot of pager apps out there the key is to get one that continues to broadcast the alert until it is read so that a response is ensured. Moreover, if the recipient of the smartphone message is unavailable when the page is originally sent, smartphone applications can ensure that the notification

[1] http://www-03.ibm.com/press/us/en/pressrelease/51067.wss

continues until read. This is not the case with pagers which are often missed if the intended recipient is unavailable or out of range.

CATALOG AND MAP EVERYTHING

The first thing you need to do is inventory your prospect's business processes. Ask your prospect to describe the company's overall business model. Then assess the contribution of each IT application to the model. This will tell you what kind of protection you need to provide and expose any related applications that will need to be protected in kind. To protect your prospective customer's business, it's vital that you take a high-level, business view of these operations.[2]

A seasoned MSP draws a lot of information on how to deal with incidents from past experiences. In order to have a catalog of all your clients past incidents you need to document them. They best way to do this is by using a ticketing system like ConnectWise that tracks the progress of the incident and everything that happens to it until it's resolved. No Incident response plan is complete without clear documentation of the policies and procedures—and personnel (including you) -- charged with carrying them out[3]. It's crucial to get customer buy-in during this phase, including provisions you'll include for testing in the near term and auditing at regular intervals.

ORGANIZING YOUR INCIDENT RESPONSE TEAM

To properly prepare for and address incidents across the organization, a centralized incident response team should be formed. This team[4] is responsible for analyzing security breaches and taking any necessary responsive measures. At its core, an IR (Incident Response) team should consist of:

INCIDENT RESPONSE MANAGER: The IR manager oversees and prioritizes actions during the detection, analysis, and containment of an incident. The manager is also responsible for conveying the special requirements of high severity incidents to the team by judging the severity of the alerts received and passing it along to the right person. In an ideal situation everyone would be on the same messaging platform with elevated alerting capability.

[2] http://blog.intronis.com/ask-intronis-how-can-i-set-up-a-disaster-recovery-plan-for-a-customer
[3] http://blog.intronis.com/ask-intronis-how-can-i-set-up-a-disaster-recovery-plan-for-a-customer
[4] https://digitalguardian.com/blog/building-your-incident-response-team-key-roles-and-responsibilities

SECURITY ANALYSTS: The manager is supported by a team of security analysts that work directly with the affected network to research the time, location, and details of an incident. There are two types of analysts:

- Triage Analysts: Filter out false positives and watch for potential intrusions. The right information can then be sent out to those managing the incident using a priority messaging app tied in with ConnectWise triggers.
- Forensic Analysts: Recover key artifacts and maintain integrity of evidence to ensure a forensically sound investigation.

THREAT RESEARCHERS: Threat researchers complement security analysts by providing threat intelligence and context for an incident. They are constantly combing the internet and identifying intelligence that may have been reported externally. Combining this information with company records of previous incidents, they build and maintain a database of internal intelligence. This is where a tool like ConnectWise comes in that allows you to catalog all the various aspects of the unfolding incident so that it can be used at a later instance to provide insight.

ON-CALL IS A REALITY – DEAL WITH IT!

Whether you have a small team or a big team. If your business requires members of your team to work unconventional hours dealing with incidents that are both diverse and random, chances are that they are not going to be too happy about this. The key to managing your team for on-call shifts is making sure everyone gets an equal share of the responsibilities while maintaining flexibility. For example, if someone has had a long and arduous on-call shift, give that person a break and shift responsibilities to someone who had a light load on their shift. Also, getting everyone in your team involved fosters collaboration. If someone needs to attend to a personal emergency then someone else on the team can take over. Having this open dialogue about on-call schedules also ensures that everyone is on the same page. It’s managements role to quantify the work done and measure who is taking on little or too much responsibility. The key here is to have management make sure that everyone participates and isn’t overloaded. Don’t dictate terms and set a schedule in stone that penalizes people when they can’t take it on.

MOVE AWAY FROM THE LAMINATED SCHEDULE – GO DIGITAL

There are apps and software out there that let you digitize a schedule. The downside to having a flexible schedule is its changing nature. The trick to managing this is to have one person on your team be responsible for creating the digital schedule and sharing it with everyone. Ideally you also want to use a digital scheduler that:

- can be changed depending on your team's circumstances
- can send out alerts to only those who are on-call on that particular day
- can program escalations if the first person on-call is occupied.

ALWAYS HAVE A PLAN B: HAVE REDUDENCIES IN PLACE

SET UP AN ESCALATION POLICY

Make sure your team is organized into an Escalation Policy. An Escalation Policy makes sure that if an incident is not acknowledged or resolved within a pre-determined amount of time, it will escalate to the correct user(s). You can customize who you want to receive the alert, the amount of time to wait before escalating to the next user(s), and which user(s) the alert should be escalated to. Those who need to receive alerts are put in one escalation group. The order in which the people are alerted should ideally be adjusted according who on your team wishes to be the first responder. Set Escalation Interval (time to escalation) and Escalation Factor (the factor that stops an escalation. Ex: the message being read) to determine how the escalation policy behaves.

SET UP A FAILOVER

In the event an alert is sent to an escalation group and does not reach anyone in the escalation group you need to have a failover policy in place that notifies either the team leader or the boss so that they can take the right actions. This can be as simple as sending an email with details of the unanswered alerts. In a post mortem of the incident, this kind of failover reporting will be useful to track what exactly happed with the alert and why it was left acknowledged.

PRIORITIZE ALERTS

Anyone who has worked an on-call shift knows that not every alert they receive is critical. To mitigate alert fatigue, it's best to classify each type of alert as high, medium or low priority. High priority alerts

are anything that is absolutely critical and must be handled to ensure business continuity. These high priority alerts are also ones that require alerting. Of course, severity of alerts is in the eye of the beholder. What is high priority for one MSP, might only be a medium priority alert for another. There is no clear, right answer on what is a high versus a medium alert. What is important however is to identify what alerts are which? Furthermore, the mindset should be that high priority alerts are critical notifications that require immediate alerting. Medium and low priority alerts can wait until the next day.

SECURE COMMUNICATION WITHIN AND ACROSS TEAMS IS CRITICAL

Communication during an incident should be conducted in a manner that protects the confidentiality of the information that is being disseminated. The incident response manager should be the central point of all communication and only those with a valid need-to-know should be included in communications regarding key incident details, indicators of compromise, adversary tactics, and procedures. Securing this communication so that Mr. Threat Actor is unable to snoop your messages is extremely vital to avoid tipping them off that an ongoing investigation is occurring. Any indication that 'you're onto them' may lead to swift changes by the attackers to further mask their activity.[5]

THE POST MORTEM

POST ALERTING

After the alert has been responded to and remediated, you need to look back at the situation and reconsider if the alert was triggered and responded to appropriately. MSPs should ask if:

- The event was triggered by a real issue or by an issue that could have waited until the following day or by an issue that didn't exist in the first place
- Was the alert delivered to the appropriate person? If not, was this because the alert was missed or was the person who received the alert unable to handle the issue?
- Was enough information provided to the MSP on-call so that they could handle the issue quickly? If not, the alerting information should to be updated so it is more robust.

[5] https://digitalguardian.com/blog/building-your-incident-response-team-key-roles-and-responsibilities

MEASURE EVERYTHING

The adage is that 'You can't manage what you can't measure.' If you want to effectively improve your response times to incidents, you need to look at historical data. Use a tool that time stamps all critical alerts and integrates that data with the platform. When metrics are immediately available, you'll be able to measure how well your team is doing, and make the necessary changes to ensure you are providing exceptional service.

ABOUT ONPAGE

We hope that these insights make it easy for you to survive your next time on-call. A lot of the tools we mention in this whitepaper are actually features of OnPage: The Complete Incident Alert Management System.

OnPage is a cloud-based, industry leading smartphone application for high-priority, real enterprise messaging. The OnPage application addresses the need for HIPAA compliant, incident response management and secure, time-sensitive messages.

OnPage takes mobile communications to the next level with the latest all-in-one app features. The web-based on-call scheduling tool enables enterprise users to plan ahead and route prioritized messages to the right person, at the right time, every time.

Thousands of healthcare providers, doctors, field engineers, law enforcement, nurses, emergency responders and disaster recovery teams depend on OnPage for rock solid reliability every day.

TO LEARN MORE, VISIT OUR WEBSITE OR CALL: ONPAGE.COM/CONTACT-US 781-916-0040