ONPAGE

SOME MESSAGES CANNOT WAIT

SECURE IT COMMUNICATIONS WHEN YOU WANNACRY

Secure IT Communications When You WannaCry

Crises communications for the cybersecurity age

On May 12th, an unknown hostile actor wreaked havoc on the British government's National Health Service as well as FedEx, Telefonica and Deutsche Bahn with its WannaCry worm. While the attack was eventually disarmed, it was not before it crippled institutions in Europe and Asia.

WannaCry and other ransomwares work by encrypting key files and then demanding ransom to unlock the files. This type of cybercrime is particularly pernicious because it brings down entire facilities and often finds victims willing to pay in order to regain access to their files. However, paying the ransom is no guarantee of having your system restored:

> Paying a ransom doesn't guarantee an organization that it will get its data back—we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom emboldens current cybercriminals to target more organizations, and offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals.[1]

Preparing for a cyberattack has unfortunately become the sort of eventuality every CISO and IT need to prepare for. While it is not something anyone wants to do, it is becoming necessary because it is no longer "if" your system will suffer attack, but "when."[2]

But imagine if IT was able to coordinate their response during a cyberattack so that the impact of business interruptions was managed? What if IT was able to continue to effectively communicate during an incident so that critical files and infrastructure could be brought back online more quickly? If the IT professionals at attacked companies had access to secure and encrypted communications, they could work around a predefined plan to bring the company back up and not be stymied by inaccessible systems.

> *The goal of this whitepaper is to:*

- Highlight the need for strong communication protocols
- Look into what a plan needs to encompasses
- Examine the components of a strong post-attack plan

[1] https://fightransomware.com/ransomware-articles/get-hit-ransomware
[2] http://www.wilkauslander.com/news-and-insights/insights/Cyber-Attacks-It-s-Not-a-question-of-if-but-when

Employ robust communication protocols

> *Practically speaking, the threat to data – both personal and corporate – is making the need for secure messaging and other options a priority for many IT professionals who are looking for newer, smarter ways to develop defense plans.*[3]

Most companies rely on internal email to communicate in the event of a crisis, despite the fact that a cyberattack might impact the email network. They also rely on fax and phone although those technologies are also easily compromised during an attack.

In using these technologies, organizations are exacerbating their inherent weaknesses and potentially providing hackers with critical company information. Instead, companies need a way to communicate during an actual cyberattack.

Ideally, the technology used in the case of an attack will be a secure, cloud-based, robust platform for communication than can be used on a smartphone. By having a cloud-based platform, the communication platform will not be under attack like the rest of the company's communications tools which are PC-based.

> *The solution [for communications during a cyberattack] is to have a critical communications platform entirely independent of the company's internal network that can be deployed in an emergency, ensuring that the bilateral lines of communication between management and staff remain open.*[4]

These prerequisites are exactly what is found in a strong smartphone-enabled, secure texting platform.

While it is important to consider the security of smartphones, it should also be noted that the security of smartphone devices is much easier to update than that of typical laptops and desktops. Security guru Bruce Scheiner noted that organizations sometimes have custom software that breaks when they change OS versions or install updates. Many of the organizations hit by WannaCry had outdated systems for exactly these reasons.[5] However, smartphones are isolated from these concerns and, with proper protocols in place, can have security updated much more easily.

Additionally, smartphones can easily enable communication redundancies which would allow messages to be received as phone messages or SMS. Also by enabling communications via data or wi-fi, there would be further enhancement of communication abilities. This would provide further assurance that important messages would get to their intended recipient.

[3] https://www.comptia.org/about-us/newsroom/blog/comptia-blog/2017/04/04/the-rise-of-secure-messaging-what-it-promises-how-it-s-being-used-and-what-it-ll-take-to-go-mainstream

[4] http://www.techpageone.co.uk/technology-uk-en/communication-vital-cyber-attack/

[5] https://www.schneier.com/blog/archives/2017/05/wannacry_ransom.html

Establish a plan

> *In this day and age, you should have a plan of action in the event of a cyber-attack. If you haven't thought about what you need to do during an attack, it's time to take a step back and rethink things.* [6]

By most definitions, a cybersecurity attack is unexpected even if businesses know that they can be a target of a cybercriminal. Given the knowledge that they could easily be a target, companies need to plan for the unexpected. More importantly, they need to consider how best to ensure critical functionality and communications in the event of a cyberattack. Readiness spells the difference between an organizations that suffer major breaches with harmful effects and an organization that will recover quickly with minimal impact.

To be sure, malware protection, network security, password security, user privilege and monitoring are important components of this culture. However, they are important discussions that need to be had *before* the attack occurs. Once the attack occurs, companies need an incident response plan to detail how teams should react and communicate. Indeed, communication is the most important part of any plan.

> *In the event of an emergency effective communication is crucial. When IT systems go down an organization needs to be able to communicate with its employees and co-ordinate an effective response. The longer this process takes the bigger impact the crisis will have.*[7]

The plan for communications during the attack need to provide for how team members will be notified and updated during the attack. Communications need to focus on

- Roles and responsibilities during the attack
- Making sure all employees are informed and alerted
- Making sure infected technologies are disabled
- Executing the disaster recovery plan

In the process of executing on this plan, teams need to use a strong incident alert management tool. An Incident Alert Management Platform needs to be able to:

- Enable secure messaging
- Provide for the ability to handle individuals and group scheduling
- Provide message escalations. If the individual contacted is not available, the message should escalate to the next individual on the schedule.
- Enable attachment of voice messages and images
- Create persistent alerting to ensure critical messages get read

By using secure messaging built-into an Incident Alert Management Platform, users have access to a communication channel that is unreadable by anyone other than the intended user and recipient. An application (like OnPage)

[6] https://www.getcujo.com/blog/the-first-five-steps-you-should-take-in-a-cyber-attack/
[7] http://www.techpageone.co.uk/technology-uk-en/communication-vital-cyber-attack/

provides end-to-end encryption to secure messages and alerts from the sender all the way to the receiver. Through this method, the confidentiality of the message remains intact at all times.

Post attack plan

> *To prevent cyberattacks from happening again, you have to understand how it happened. The best way to effect this outcome is to launch a post-mortem review[8].*

A post-mortem analysis should be part of your incident response plan. Teams should schedule a post-mortem as soon after the incident as possible so that recall and responses taken are not forgotten.

A security incident can be a galvanizing event that provides the momentum to improve incident response plans, fix flaws in your processes and harden your defenses against a community of cybercriminals who are constantly refining their skills and techniques. By having a post-mortem, businesses can translate that energy into a positive working plan to protect against future attacks.

After the attack has occurred, there needs to be a concerted effort by the team to see what went right and what needs to be changed for next time. For example, teams should ask:

- How long did it take until we were able to access back-up files?
- Were employees able to communicate during the attack?
- Did employees have cancel important business because of the attack?
- What business routines were impacted?

By answering these questions, teams can improve their practices for security and communication for next time and increase their resilience. Indeed, while another attack is always around the corner, it does not need to be a given that the cyberattack overwhelms the business and shuts it down.

Conclusion

Cybersecurity incidents are a persistent menace. Businesses need to consider incident response plans that address the possibility of degraded operation while also considering how to achieve an efficient restoration and recovery. Clearly, maintaining strong communications during the course of the cyberattack is an important part of returning to business as normal. To achieve this goal, businesses are best served by employing encrypted cloud-based communications.

Furthermore, by having secure texting and messaging communications enabled on smartphones, companies and their IT will be less adversely effected by any cybersecurity attack and can continue on a quick path to remediation.

[8] http://blog.demisto.com/the-top-seven-steps-for-conducting-a-post-mortem-following-a-security-incident

About OnPage

OnPage is the industry leading Incident Alert Management System. Built around the incident resolution life-cycle, the platform enables organizations to get the most out of their digital investments, ensuring that sensors and monitoring systems have a reliable means to escalate abnormality alerts to the right person immediately.

OnPage's escalation policies, message and alerting redundancies, and scheduling algorithms ensure that a critical message is never missed. These features are all a part of the three components that make up The OnPage Platform: The Alert Engine, The Escalation Manager and The Postmortem Reporting. Click here to learn more

Visit our website or call: ONPAGE.COM / 781-916-0040

Visit iTunes or Google Play from your smart phone or tablet to download the OnPage app.

Available on the App Store

Get it on Google play