CISO GLOBAL

eBOOK

10 Truths

That Will **Change** How You View **Cybersecurity**

Author: **Chris Clements**
VP of Solutions Consulting

Table of Contents

© Copyright 2023 CISO Global. All rights reserved.

Lessons Learned from Watching the Incident Response Team

As we look back on Cybersecurity Awareness messaging over the last year, many of us who are seasoned practitioners are excited to see security becoming more top of mind for end users . That said, it seems many best practices highlighted during these campaigns – while true and valuable – miss the heart of what experts see on a daily basis when mitigating real world attacks. There are some practical life lessons that will make a major impact on how organizations approach their security programs – ten, to be exact. CISO Global is in the fortunate position of having insight into the security practices of diverse organizations. Many, including a great number of those with professional IT departments, don't realize how quickly an attacker can gain access to their networks, or how fast they can navigate quietly into more sensitive systems. IT Security has always been seen as a game of cat-and-mouse between attackers and defenders – an electronic arms race. Attackers have the same tools at their disposal as the defenders, meaning attacks can be refined until they bypass defenses. For example, if an attacker wants to bypass antivirus, they can simply install all the common anti-virus software and test their code against that software to see which code variations are not detected.

Working on the front lines with the CISO Global Incident Response (IR) Team, I have the benefit of having gained a great deal of insight into how attackers operate. Here in, I'm offering you some real-world advice that can help reduce the impact of an attack.

First lEt's address the biggest elephant in the room:

1. The Hacked Company on the News Could Have Been You

A company that gets hacked isn't necessarily doing anything worse than other typical companies. In this day and age do you think it was because the hacked company was doing something like not running antivirus? Of course not, they are probably doing much the same things you are. Companies need to defend against all security vulnerabilities, while attackers only need to find one vulnerability to get initial access. The larger an organization, the more complex the IT environment; the larger the attack surface, the harder it is for an organization to manage and control it.

It's time to adopt the mindset of: "when", not "if" an attacker gets initial access.

2. It's a Question of "When," Not "If" an Attacker Gets Initial Access

Though it does happen, the majority of cyberattacks today don't begin with attackers hacking into an external firewall. The most common attacks today are users being targeted through phishing emails. There are many great anti-phishing technologies and end-user training programs, but no solution is 100%. Sooner or later, an attacker is going to craft an email that will get successfully delivered to an unsuspecting user's inbox. Eventually, a user will fall for the lure and take an action that gives the intruder initial access, whether by disclosing their account credentials or running the attacker's malware. There is a misconception that endpoint anti-malware solutions are impossible to bypass. Sophisticated cybercriminals can often sidestep protections, and their success certainly varies from vendor to vendor, but, no product is a silver bullet that will catch all threats and malware all the time.

Companies need to prepare for a successful attack by implementing layered defenses that limits and mitigates threats. The old comparison is that of a submarine being not just one big hollow tube, but rather many compartments that can be sealed off in a breach or failure.

3. File Encryption and Ransom Demands are the LAST Steps in an Attack, not the First

Many people believe that malware payload detonation immediately triggers file encryption. In fact, what happens is that the attacker uses the initial malware payload to get a toehold in the environment, then expands into the environment and attempts to elevate privileges. The attackers then exfiltrate as much of your data as they can. Their goal is to stay in the environment until it serves no further purpose. If they are caught or have all they need, they will detonate the ransomware and leave. This means it's unlikely that a ransomware attack on your environment will be isolated to a single system. By the time you get files encrypted and a ransom note, it's the final phase of the attack, not the initial. The attacker could have been in your environment for 3-6 months.

Diligence must be paid to logging, auditing, active alerting, dubious network connections, DNS name resolutions, and anomalous user activity.

4. Geofencing Actually Works

Blocking communications to countries you don't do business with can help thwart an attack. My prior belief was that geofencing was a lost cause because an attacker could use a VPN to appear to be from the country or city of the victim. What I've seen happen in real life is geofencing working as designed. It's possible that this is due to the initial ingress being automated with the attacker using internationally hosted servers. A user will fall prey to a phishing attack, or another attack that compromises credentials or session tokens, and the attacker has every piece of information they need to login as the victim. However, the logs will show a rejected login attempt from Russia, China, or another country, blocked solely using the location of the attacking system. It's not perfect, but it's another layer in defenses.

If your company doesn't do business internationally, limit access to your local country, or countries that you do business with. Ensure both inbound and outbound traffic is geofenced. If you have staff who travel, whitelist those that specific users to a specific country while they are away or have them use a VPN solution for remote access.

Companies need to prepare for a successful attack by implementing layered defenses that limits and mitigates threats.

5. Send All Logs into a SIEM for Analysis

If you aren't sending logs to a central location and doing analysis, you'll be missing important signals and lack visibility that attacks are happening. Many organizations believe that simply turning on logging at the device is good enough. This is untrue for several reasons. If that device is compromised, the logs can be tampered with or erased. If there is an incident, analysis is slowed, as the IR engineer needs to go to every device individually; this is time-consuming work, and time is money. Isolated logs can't be aggregated or events be analyzed as a whole.

Logs are key to knowing that something is awry in your network and log review is a proactive measure to detect malicious activity as well as assist in analysis if there is an incident.

6. Multi-Factor Authentication (MFA)

It is not an understatement to say that almost every organization has some type of cloud presence, whether email or Azure Active Directory. Moving any type of internal IT function to the cloud changes the security boundaries; what was previously protected by corporate security infrastructure is now accessible and attackable by every hacker in the world. This places extra onus on authentication security, since it will be stressed and tested almost continually. A fundamental requirement in this new world is Multi-Factor Authentication (MFA), also referred to as Two-Factor Authentication (2FA).

Many companies are resisting this move to MFA because it's seen as an inconvenience, but there is no doubt that delaying is a risky proposition. We have seen companies that have had Domain Administrator accounts overtaken and, in one month, had tens of thousands of dollars of cloud compute resources created by an attacker to mine cryptocurrencies. Enabling MFA would have almost assuredly prevented this loss.

At minimum, every privileged role MUST have MFA enabled, and MFA should be enforced for every user on any cloud-based service like Microsoft 365 (or any locally hosted service) where authentication is exposed to the Internet. Given the ubiquitous nature of MFA, there is no real reason why every user should not be using MFA. There are always arguments and articles about what type of MFA mechanism is the best, but in reality, every single solution is 1,000 times better than having no MFA at all.

7. Network Segmentation and Isolation; Contrasting Extremes

Imagine an unfortunately common network configuration that has every single device in one large internal network with a Firewall protecting it from direct inbound attacks from the Internet but allowing any traffic outbound. On this network, every system can contact the management ports for the firewall, printers that haven't had the firmware updated in a decade, servers, and a myriad of other IoT devices like cameras and thermostats, embedded systems, and lab machines that can't be patched on any regular schedule. Not to mention the fact that every user's desktop can talk to every desktop and server in the organization, whether on-site or remotely connected over a VPN. A hack or infection in this environment provides a myriad of attack vectors that an attacker can leverage across the entire environment using the unfettered internet access to report back to the "Command and Control" (C2) servers. This is literally an attacker's paradise.

It is possible the entire attack is essentially stifled before it escalates. Proper logging and SIEM configuration would be sending many serious alerts very early on!

Conversely, imagine the opposite extreme, a "compartmentalized" network, which is a good standard to strive for in the future. This network would look something like this:

- Devices with management ports are put on an isolated management network that can only be contacted by people manage the devices.
- Embedded devices like cameras and thermostats, are separated onto their own network with strict rules that allow management and software updates only. They are not trusted and, therefore, have no need to communicate with any business resources.
- Servers have no outbound access to the Internet except to specific sites needed for updates, but user systems can connect to them only in the manner needed for business. If users need to access a web application, then all other access is blocked except to the specific web service. Access to other ports like Remote Desktop Protocol port is unnecessary for normal users
- User systems can browse the Internet but cannot contact any other internal systems apart from the specific servers and services needed for that job role. Access to services and servers is limited as much as possible; (e.g., A finance user doesn't have access to Engineering data).

- The firewall filters all traffic, brokers all inbound and outbound traffic, and blocks communications to known bad sites and countries where business is not conducted.

- A VPN user only gets access to the specific resources needed for the role, not every system on the network.

In the above this scenario, which is essentially based on "the principal of least privilege", an infection on a user's system has limited ability to spread within an organization, has no easy targets, and hopefully any "phone home" communications will be blocked at the firewall. It is possible the entire attack is essentially stifled before it escalates. Proper logging and SIEM configuration would be sending many serious alerts very early on!

Proactive analysis of an environment can find issues before they become a fully fledged emergency.

Unfortunately, the second compartmentalized configuration scenario is rare because network architecture evolves, or devolves, over time, and it becomes just an inherited system that is too difficult, or too costly, to change when it's working well enough. If your network looks more like the first open configuration scenario, consider steps to move toward the compartmentalized configuration. Quick wins can be made by creating a management network and isolating vulnerable management interfaces, along with isolating embedded systems as well as systems that can't be patched, protecting them with strict firewall rules. The next step is to create functional subnets for servers and users. These networks can be subdivided by role. Finance and HR are separated from IT and Development. Similarly, firewalls on endpoints could be programmatically configured (e.g., via a GPO), to only allow endpoint traffic to required servers and not every other system in the environment. Server networks can be divided by web/application servers, API services, data warehouses, and backend services. This model allows a compromise at one layer from spreading to the whole environment.

8. Proactively Run Threat "Hunts"

Proactive analysis of your environment that includes hunting for potential threats and vulnerabilities in your system can find issues before they become a fully fledged emergency. Searching for known Indicators of Compromise can also allow tuning of security products to catch them in the future and to understand the possible gaps or limitations in the controls you have implemented.

Knowing the legitimate software in use in your environment is valuable. Attackers now routinely leverage legitimate remote access software like teamviewer and gotomypc for Command and Control. They know it's highly unlikely that any anti-malware software will flag them as malicious, since they are often used for legitimate business purposes, and

it still gives them complete control over the compromised system. Proactively hunting for new installs of remote-control software that you did not install can both alert to an external attacker's presence as well as identify policy violations by internal users.

9. Users are Now the Most Common Cause of a Successful Malware Attack

Statistically, a user performing an action such as opening a poisoned attachment, clicking on a bad link, or getting phished is going to be the way an attacker enters your environment. The degree to which you can educate, protect, and compartmentalize a user will dictate your level of resilience to attack:

- Educate users on how to determine potentially bad emails, websites, and attachments. This should be an annual exercise. I've seen compromises caused by a user opening and clicking on where a user literally opened and clicked every email they received regarding fake Amazon gift cards, theatre tickets, everything. These types of emails are the easiest to detect; so just imagine if the user had been sent a targeted attack that looked like an IT email asking to change their password on the new application portal. Use a security awareness training program to teach users to be diligent and question everything they receive in an email or download.

- Protect users from receiving malicious emails or attachments. Implement and configure aggressive filters on email with explicit warnings inserted into inbound email originating outside the organization. Implement end-point protection and antivirus software as a last line of defense. Use a high-quality web filter that can use advanced methods to detect sites used to push phishing payloads.
- Restrict employees to infrastructure and systems that are needed for their job role. In the case of a successful attack, this hopefully will limit the damage and will not spread throughout the network.

10. Create An Incident Response Plan

Every organization should have an Incident Response Plan that details what constitutes an incident; who gets contacted internally, from executives to legal counsel, who handles any PR issues if needed, how an incident is initiated with vendors, etc. Too often there is confusion around who has what roles and how to engage external teams, causing unnecessary delay. Your IR plan should be executed as a table-top exercise annually.

Hopefully the insights above, gleaned from real Incident Response projects, will help you reflect on how your environment might cope with an attack. When you understand how hackers and malware operate, it will help you understand what refinements support quick recovery and better outcomes. It helps to use a mindset that a successful attack will happen, and when it does, you will be prepared with a step-by-step Incident Response plan that will help to minimize the damage. If the detonation of malware is a spark from a fire, will it burn your environment down by landing on kindling and starting a wildfire?... or will it be like a spark that lands on a lake and is quenched in an instant?

About CISO Global

About Us

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, security engineers, and around-the-clock analysts.

To learn more, visit www.ciso.inc.

CISO GLOBAL

480-389-3444 | ciso.inc