SOLUTION GUIDE

Five Lessons for Security Leaders from the Past Year's Breaches

CYCOGNITO

It's been a challenging—and, at times, frightening—year for cyber security pros with an array of high-profile breaches that have disrupted business operations, broken down supply chains and even led to business shutdowns. We've seen sophisticated attacks on governments by state-sponsored entities. We've seen a decided increase in ransomware shutting down core infrastructure. We've seen supply chain breaches that impact hundreds, if not thousands, of downstream organizations. So what do the recent attacks tell us about the state of security today and how can we learn from them?

Five Lessons for Security Leaders from the Past Year's Breaches

Here are our top 5 lessons for security leaders from the past year's major breaches. We hope this helps enable a more secure future for your organization.

Key lessons learned:

01
Solar Winds
Watch your supply chain

02
Colonial Pipeline
Secure your remote access services.

03
Microsoft Exchange
Don't forget your old IT equipment

04
Accellion FTA
Communicate early and completely

05
Water Utilities
Stay vigilant

01

LEARNED FROM SOLARWINDS

You need to know what IT assets you own and where they are, because attacks can come from anywhere—including the supply chain.

THE FACTS: In December 2020, cybersecurity firm FireEye announced they'd been the victim of a successful attack where their own Red Team toolkit was stolen; later that month FireEye informed SolarWinds that attackers had gotten into their systems via a backdoor planted in SolarWinds' Orion software update. APT29, a nation state actor associated with Russia intelligence agencies, essentially weaponized SolarWinds' commercial software by embedding malware in the Orion update and allowed the attackers to use the code almost as a form of trojan, getting into every device and system it's configured to monitor and manage.

Lesson learned from Solarwinds

Attacks can come from anywhere, even the most trusted vendors in your supply chain, like SolarWinds. This is especially true when those vendors are targeted by highly sophisticated, state-sponsored actors. That's why it's vitally important to know what IT assets you use and where they are. Having the knowledge of your assets, who owns them, and how critical they are to the business lets you respond quickly to risks to those assets.

For the SolarWinds breach, if those impacted knew their attack surface, including the supply chain, then the moment that they were made aware of the breach they could see if they were impacted. This is in stark contrast to the hours, days, weeks that it might otherwise take.

"Attackers understand that your IT ecosystem extends well beyond your own organization and that you don't control the security of all of your supply chain participants. They also know that organizations don't have an easy way to discover all of those IT assets and test them for potential attack vectors. The SUNBURST attacks demonstrate organizations can be blindsided by unseen security weaknesses and vulnerabilities they simply don't know how to find, let alone resolve."

Read our full write-up on the SolarWinds supply chain attacks.

02

LEARNED FROM COLONIAL PIPELINE

It's time to focus on finding remote access services to protect against ransomware.

THE FACTS: In early May of 2021 ransomware group DarkSide shut down 5,550 miles of petroleum pipeline, stranding barrels of gasoline, diesel and jet fuel on the Gulf Coast of the U.S. It appears that hackers gained entry via the company's VPN **using a compromised password**. The group has been operating their ransomware—called "DarkSide ransomware" and delivered as-a-service – against U.S. and European companies for at least half a year. Attackers using DarkSide's ransomware variant generally gain initial access by exploiting remote services like Citrix, Remote Desktop Web (RDWeb), or remote desktop protocol (RDP) from an external attack surface. Once they gain a foothold, they dig in deeper via lateral movement, exfiltrating data, and then encrypt everything with ransomware to extort money from their victims.

Lesson learned from Colonial Pipeline

Successful ransomware attacks are big business – even given that some of the Colonial ransom money was returned. The ROI for attackers of ransomware attacks like this one was **estimated at 1,400%**. Typically these attackers perform reconnaissance, then, as noted earlier, they access the target via some type of remote access service. Then they go lateral to find and encrypt valuable assets. The pandemic has made it easier than ever for groups like DarkSide to find targets.

Once attackers locate a target, they may buy access credentials on the Dark Web, or rent a botnet to brute force the system. The thing to remember is that the remote access service that will be targeted is likely one that you have forgotten about or never knew about in the first place. Maybe your company acquired another organization that had its own subsidiaries, and an employee of one of those subsidiaries set up an RDP server. Maybe the pandemic required remote access for server administration.

Ransomware attackers have become quite sophisticated this past year, "segmenting the market" and running large-scale campaigns against small and mid-size organizations, and more targeted campaigns against large organizations or those with mission-critical operations (i.e., hospitals, oil pipelines and local governments). Large companies, particularly those that have a history with acquisitions, mergers, or partnerships are an appealing target because of their complex IT ecosystems.

Given the confluence of big business and big dollars for attackers in ransom payments, the best defense is to ensure that you find and secure remote services. While this is easy to say, we know from experience that it's difficult to actually do without an external attack surface management solution to provide visibility, offer insights and help set priorities.

"Our research at CyCognito finds that about 1 in 65,000 assets in a typical Fortune 500 company will contain an unprotected remote desktop service. That may seem like good odds, but at-scale this means most major corporations are hosting between two to twenty or more easily exploited systems, right now!"

Read our full write-up on the Colonial Pipeline ransomware.

03

LEARNED FROM MICROSOFT EXCHANGE VULNERABILITIES (OLD AND NEW!)

Don't forget your old gear... because attackers won't.

THE FACTS: A number of vulnerabilities in Microsoft Exchange Servers have turned up in 2021. Some, including CVE-2021-26855, -26857, -26858 and -27065 are Remote Code Execution (RCE) Vulnerabilities targeting 2010, 2013, 2016 or 2019 servers. The vulnerabilities were reportedly used in multiple Zero Day exploits, in which they were used to gain access to email accounts and to plant additional malware.

Because all of the vulnerabilities mentioned above are RCEs they allow an authenticated attacker to write a file to any path on the server. While these flaws have likely been around for a long time, exploitation of them took off in January along with the press coverage. A sophisticated group of attackers out of China dubbed Hafnium initially used these vulnerabilities, but then as soon as it went public it became a free-for-all. Over a matter of days the number of potential victims went from 30,000 to 60,000 or more.

Lesson learned from Colonial Pipeline

As you can see, some of these are for older systems, and in the case of the MSE 2010 servers, hardware/software that is no longer supported by Microsoft. The number one lesson here is don't forget your old gear... because attackers won't. You should be continuously monitoring your entire external attack surface for security gaps, even on the older gear. Yes, it's absolutely imperative that you monitor the newer technologies that power digital transformation like cloud and SaaS applications, but this set of vulnerabilities is a reminder that it's in monitoring the combination of the new and the old that we find true security.

In addition, even if your company has upgraded or replaced systems that are at risk, you must not assume that everyone that you do business with has followed suit. A small subsidiary of one of your third-party suppliers may not ever think of replacing a server that's working "perfectly well." Ditto for your partners.

"It's easy to get caught up in the shiny, newness of the technology landscapes we create during this age of digital transformation. So this zero-day is a great reminder that while newness is certainly important—we also need to keep looking for those aging systems that may be tried-and-true, but need to be upgraded or replaced before they are forgotten paths of least resistance."
Read our full write-up on the MS Exchange vulnerabilities.

04

LEARNED FROM ACCELLION FTA-RELATED BREACHES

Brush up your breach disclosure policy and be sure that when confronted with a problem (like a breach), you tell the whole truth.

THE FACTS: Accellion engaged FireEye Mandiant in March 2021 to investigate earlier attacks on their legacy File Transfer Appliance (FTA). Accellion, which had quietly issued a patch in December while emphasizing the end-of-life for the equipment, failed to point out the severity of possible exploits. The attack used a combination of zero-day attacks to insert a new web shell and extract data which was then held for ransom. The attackers, identified as CloP, then began to issue extortion letters in January. Victims were customers and even the customers of Accellion customers, including major financial and healthcare institutions, as well as a number of universities and global retailers.

Lesson learned

One of the biggest lessons learned from the Accellion breach is one that your Mom may have taught you: Tell the whole truth. The most consistently reported topic related to the breaches (along with "don't forget your older gear") is that Accellion tried to downplay the issues and consequently gave themselves a black eye. Breaches continued to emerge months after the actual exploit because organizations didn't have the right info on how to prioritize the risk.

This series of events also serves as a reminder that it's best to have forthright breach disclosure rules in place before a breach happens. And, again, it's important to fully explain what went wrong.

"This [the Accellion FTA-related breaches], on top of other recent supply chain hacks, led me to think about the importance of communication when these breaches happen: What good looks like. And what it doesn't. With the Accellion breach(es), I found that not all disclosures were public or full or timely, and some weren't any of those things. Let's take a look at why that's a bigger problem than this one supply chain attack."
Read our full write-up on the Accellion FTA-related breaches.

05

LEARNED FROM FLORIDA AND CALIFORNIA WATER UTILITIES HACKS

The stakes continue to go up so it's important to stay vigilant.

THE FACTS: In February 2021 a water treatment plant employee in Oldsmar, Florida noticed that someone else was remotely controlling his computer. Apparently this behavior in itself was not alarming given remote access is commonly employed to troubleshoot IT, but what was alarming was the person on the controls tried to turn up the amount of lye (sodium hydroxide) in the water to dangerous levels. Fortunately, the employee was able to act quickly and mitigate what could have been a dangerous and life-threatening breach.

Meanwhile, unbeknownst to the world, in January 2021 another water system, this time in San Francisco, California, was similarly compromised. Again, the water utility was accessed by the attackers using an employee account in TeamViewer, third party software which allows connectivity between computers for remote access. The attacker, once logged in, proceeded to delete programs for treatment of drinking water. The attack was discovered quickly—the next day—passwords were changed, and the general public did not hear of the attack until months later.

Lesson learned

This last batch of threats are designed by attackers to inspire fear, as they target a piece of lifesustaining and critical infrastructure—water utility systems. Combine these with the Colonial Pipeline shutdown of a key U.S. oil pipeline and ransomware attacks on hospitals and we see that there does not appear to be a moral or human limit to what attackers will do, and what systems they are willing to shut down if they are not paid. In this atmosphere, it's important that security leaders continue to stay vigilant and do everything they can to prevent attackers from getting into their systems in the first place.

Make Sure the Next Story Isn't About You

One of the commonalities of these lessons is that they involved vulnerable or unprotected software or systems that attackers were able to find and exploit. The solution might seem simple—just protect everything. The reality is much more complicated.

Today's IT environment is extraordinarily complex, with remote access services, software and systems that are not new but are still in use, and an intricate chain of partners, suppliers and subsidiaries. And, of course that's not all. In many cases, attackers can access organizations via routes that cyber security staff cannot protect because they are unaware that such routes exist. Breachable assets could belong to supply chain vendors, or even to those vendors' vendors. They may have come from a well-meaning staffer that needed to solve an immediate problem then forgot to mention a new cloud service to IT. And sometimes the means to infiltrate an organization could originate with gear so buried in historical operations that the organization has just forgotten that it exists.

No matter the origin of your breachable points, and regardless of the size or your organization, your actual attack surface is almost certainly much larger than you think. In order to protect yourself well, you need to be able to identify your real vulnerabilities, and the only way to really do that is to see your organization through the lens of an attacker. Once you know what your actual attack surface looks like, you can prioritize your defenses, and stay out of the headlines.

Attack Surface Protection with CyCognito

The CyCognito platform provides proactive security that can help protect you from the types of data breaches described in this post. It preempts attacks and helps you operationalize common security frameworks like MITRE ATT&CK and aligns with regulatory compliance standards. The platform achieves this by discovering and testing your entire attack surface, prioritizing what needs to be fixed first, integrating with and orchestrating existing workflows, as well as automatically validating remediation.

Interested in learning more? Watch a short demo video now.

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO