www.pipelinepub.com
Volume 20, Issue 7

Cybersecurity Risk Nobody is Prepared For

By: Kim Scott

For CEOs it's a recurring nightmare: waking up to a call saying, "We've been hacked." How did it happen? "We don't know. We've never seen this before." This bump in the night is happening frequently. GenAI is going to accelerate the appearance of these previously unknown attacks. While some technology tries to target unknown attacks, our defensive tools are best at protecting from known threats. A new set of tools is needed. These tools need to both find and remediate the unexpected attacks. Technologies implanting fine grained, non-centralized, behavioral analysis, and dynamic low latency remediation will be the key foundations of these tools.

Examples of Unexpected Attacks

The MGM casino 2023 attack resulted in estimated costs of $100M. How it happened is still not fully known or publicly shared, but it's been widely shared that the attack started with Phishing ploy that gave the attackers credentials needed to deploy their ransomware. Most of today's tools struggle to detect these types of attacks as they tend to resemble normal operations.

Recently, Microsoft Azure announced an attack where the hackers were able to take over targeted accounts using credentials obtained through phishing techniques. There is suspicion that the attackers may have updated Multi-factor Authentication (MFA) information to enable them to remain resident in the systems longer. This type of attack is difficult for today's technologies to detect quickly. Often an attack of this type isn't detected by a cyber security monitoring tool, but rather through a series of end users reporting unexpected system behaviors.

Not all things that go bump in the night can be attributed to known causes. In May 2024, AT&T announced that about 70 million current and formal AT&T clients have personal information such as Social Security Numbers and/or pass codes on the dark web. They haven't yet announced how the data was exfiltrated or even if the data came from AT&T or one of AT&T's vendors. At the time of this writing, AT&T has shared that they are still investigating.

Sometimes it's not a specific business that's targeted, but rather a tool. For example, the MOVEit file transfer service attack targeted a zero-day vulnerability that opened the door to an SQL injection attack. No one expected that the file transfer service that was in common use across enterprises —

government, education, etc. — could be exploited. One source estimates that the MOVEit attack has already affected over 1,000 organizations and 60 million individuals worldwide.

An executive can wake up to an attack on a totally different organization resulting in the crippling of their organization. In February of 2024, many health care providers, hospitals, pharmacies, etc. woke up to find that they weren't going to get paid. The non-payment wasn't for anything in their systems, but because Change Healthcare Group (a health care payment system), had been crippled by a ransomware attack. As of this writing, many health care providers have still been forced to lay off staff and restrict services. Once the information has been encrypted in a ransomware attack, restoration operations can be expensive, time consuming, and often not fully successful.

In these examples, multiple vulnerabilities were leveraged to breach the system. While today's solutions do a reasonable job correlating data across security technologies, monitoring solutions tend to sample data due to the vast quantities of security alerts. Centralized monitoring solutions may correlate information over time to detect anomalies. However, tools leveraging such strategies tend to insert latency into the detection process which can cause expensive delays in detection or detection after it's too late. In addition, the tools are reliant upon the data sampling choices and may miss important information.

Detection and Defensive Approaches

In the examples above, several common deficiencies were exploited. Social engineering, phishing, and poor security hygiene were all cited techniques used in the exploits. It's not publicly known what caused the AT&T hack at this time, as the company is still researching and hasn't released information regarding their investigation.

With the millions of dollars per year spent on cybersecurity, why are these attacks still difficult to detect?

Social engineering attacks target employees by leveraging their inclinations and convincing them to give attackers what they need for access and control. Often, there are security gates in place, but the attackers create a sense of urgency persuading the
employees to bypass the gates. These attacks aren't visible to typical security technologies because they look like normal activities. However, there are techniques similar to the multi factor authentication used to protect fraudulent logins that could be used to detect social engineering attacks. For example, process changes could be employed to require multiple approvals for certain actions. Similarly, code could be written to defer credential changes until they could be authorized by separate functions.

A good first step would be to audit key processes to determine which ones are protected solely by company policies. Some of those policies should probably be candidates for additional protections.

This would reduce the social engineering attack surface, but in order to thwart an attack in progress, monitoring at a different level is required. A common practice today is to correlate and monitor logs across a spectrum of security technologies such as firewall, endpoint detection and response (EDR)'s, etc. In order to detect social engineering, monitoring could be done across applications to detect atypical process executions. For example, if account credentials are typically done with new hires, or promotions, actions could be fired when typical HR platforms aren't set up before new credential requests. Businesses could start making cross checks on credential updates as well.

In these examples, the attacks became more expensive the longer they remained undetected. Monitoring technologies that ingest logs in a central site system, and then correlate them for anomalies, introduce latency in order to spot patterns. Alternatively, social engineering introduces

latency because those attacks tend not to look abnormal until much damage has occurred. This gives rise to the need for low latency solutions that can correct issues before they have a chance to spread their infection, extract more data and increase expense.

Solutions that are non-centralized can reduce the latency issue. One implementation of such a solution may have specialized monitoring resident on the end points, servers, Clouds, applications, etc., that would not only be able to alert more quickly but could have remediation capacity as well. For example, routines could be set up to block a user, restore from backup, or any number of activities as opposed to just alerting. Many businesses are cautious about automating remediation as they are concerned about unforeseen circumstances, but small changes can be a life saver in certain situations.

In many of the examples above, the attackers were able to install malware after cracking through the first level(s) of defenses. While malware varies, the intent could be to extract information, spread infection, create damage, or perform any number of harmful exploits. There are technologies today that can detect some of these situations and give the network defenders a chance to remediate. Since the amount of damage increases consistent with the amount of time the malware operates, automated remediation should be considered. Some situations may be good candidates to automate.

Finally, the attackers are continuing to innovate, and situations like AT&T's recent attack are not uncommon. Much time has passed, and yet the existing technology and practices in place are still struggling to figure out what happened. State of the art technologies sifting through huge data lakes of logs to try to find anomalies may struggle to see these zero-day attacks because there may not be signatures yet for identification, or they may be lost in too large a sea of data. Smaller algorithms running closer to attack entry points might be more helpful since there would be less data to sift through, thus making anomalies quicker to spot. These algorithms could also be permissioned to take defensive actions, alert quicker, and provide faster, more tailored renditions than a more centralized approach.

Conclusion

Businesses are allotting more and more of their budgets to cybersecurity. Yet, in spite of greater investments being made in security, attackers are still getting in, leveraging vulnerabilities, and innovating new approaches. Most executives fear that while they're doing all they can, they will inevitability fall victim to an attack. The fact that attacks on large enterprises such as AT&T, MGM, and Microsoft Azure have been in the press makes those bumps in the night all the more concerning to executives.

As attacks continue to evolve, it is increasingly important for organizations to examine their processes to determine where they are vulnerable to social engineering. It is also important to diversify and automate defenses, and to not only leverage today's centralized monitoring solutions, but to also add non-centralized monitoring.