CUSTOMER CASE STUDY

Attivo NETWORKS

DUE DILIGENCE: DECEPTION TECHNOLOGY IN MERGER AND ACQUISITION SETTINGS

Merger and Acquisition (M&A) activities inevitably lead to a range of changes across the newly combined organizations in structure, management, and technologies. The challenges of merging business cultures and processes can be daunting and are often compounded with the technical challenges of integrating business networks and their attendant topologies, policies, and security infrastructure. This white paper will delve into some of the information security challenges organizations are likely to face during the M&A process, and how using deception technology to identify potential issues will make the infrastructure integration process smoother and more secure.

CHALLENGES

Merging organizations presents a myriad of challenges. In many cases, one of the organizations involved has an information security infrastructure that is considerably more mature and evolved than their new partner. At the most basic level, due diligence requires a review of existing policies and procedures. However, best practice calls for a much more thorough vetting of the new acquisition's environment before they are integrated, especially to verify that their networks haven't been compromised.

For example, one of Attivo Networks large retail customers had grown both organically and through M&A. They had developed a mature security model that featured process, procedures, and technologies, designed with industry best practices in mind.

An ongoing challenge was assessing the security controls on their affiliate organizations and new acquisitions. The major concern was that the affiliate network didn't meet their enterprise standards and lacked the maturity or defenses to quickly detect and mitigate cyberattacks. Specifically, they were concerned that the acquired networks had hidden or time-triggered malware that could move laterally across merged networks, potentially breach their corporate network, and lead to the exfiltration of company and customer data.

This situation is relatively common, in that organizations frequently have different security paradigms. The maturity of each organization can vary, of course. But the end goal is the same: bring both companies to the same high level of security and preparedness.

THE ROLE OF DECEPTION

The earlier the Information Security team gets involved in the network integration process, the more benefit they can provide in the process. The security team's primary goals are to assess the networks, processes, and procedures of the new environment to assess whether they meet the standards set by the parent enterprise. How the InfoSec team evaluates the newly acquired network depends on the specifics of the merger, but audits, threat scans, and penetration tests are common.

Another task for the InfoSec team is determining if there is are any existing compromises in the new environment. This was of primary concern for the reference organization here, as their industry (retail sales) had suffered several high-profile incidents in the recent years and they did not wish to suffer a similar compromise.

While "dwell time" – the time between an initial compromise and the attack's discovery – has dropped consistently over the years, it still averages over 100 days globally between intrusion and detection. As attackers have become more sophisticated and highly targeted attacks have grown more common, organizations have faced greater challenges identifying threats on their network. This presents a unique challenge for the team assessing the new network, as any compromises already in the network demonstrate that they had managed to avoid detection by the existing security tools. In fact, an attacker inside the network may have gained control of the very systems designed to keep them out.

Organizations frequently have different security paradigms. The maturity of each organization can vary, of course. But the end goal is the same: bring both companies to the same high level of security and preparedness.

This is where deception technology provides the Information Security team the tools they need to get visibility into the environment and to proactively lure hidden attackers out of hiding. Placing realistic deception throughout the network, as both network decoys and attractive lures, such as deceptive credentials and other assets, provides

detection of threats that perimeter defenses have missed. Once inside the network an attacker with reasonable skills will have relatively free reign to scout, harvest credentials, and establish a foothold. Deception technology changes the game by altering the attack surface in favor the defender. The preemptive deployment of traps and lures will deter and misdirect attackers and drive them to make mistakes that will reveal their presence.

Since any touch on a decoy server or service is suspect, as is the use of deceptive credentials or accessing decoy assets, the assessment team will receive high fidelity alerts to events other systems may have missed. Even skilled attackers who are moving "low and slow" to avoid detection by existing defenses are likely to trip a deception alert because they are unable to distinguish real assets from the deceptive environment and even the lightest ping will trigger the alarm.

The ability to detect skilled persistent attackers is what led the example organization to choose deception technology for their Mergers and Acquisition assessment efforts. They considered it the best choice to provide accurate detection and deep visibility into the networks they were assessing, without adding excessive overhead and time to their engagement. Other techniques, such as threat hunting, were too resource intensive in both time and assets for their needs.

The ability to detect skilled persistent attackers is what led the example organization to choose deception technology for their Mergers and Acquisition assessment efforts.

HOW ATTIVO NETWORKS COMPLETES THE PICTURE

The Attivo Networks ® ThreatDefend™ platform provides the flexibility, scalability, and ease of use needed to quickly and accurately detect attackers that may exist in an environment. By deploying deception into an environment, the Information Security team can establish a proactive defense designed to detect and derail attackers on the network. At the same time, they will improve the overall security posture to thwart future attacks before they can progress beyond the initial compromise.

The large retailer referenced earlier implemented the full range of the ThreatDefend™ platform in their M&A efforts, deploying a scalable, light weight, highly effective, solution across their subsidiaries. The BOTsink® server provides decoy systems and services that are indistinguishable from the company's production assets. These decoys present an attacker with attractive targets that engage, trap, and safely record an attacker's tactics, techniques, and procedures. They added the ThreatStrike™ solution on the endpoints to detect credential-based attacks and identify

attacks against shared assets. These decoy credentials integrate with Active Directory to appear authentic, while only granting access to decoy systems that will immediately identify an attack. The retail organization used the ThreatDirect™ solution to project decoys into remote locations with minimal overhead, making their M&A efforts more efficient and more economical. Finally, the ThreatPath™ solution identified potentially vulnerable access pathways before they could be compromised.

The organization successfully deployed the ThreatDefend™ platform in their enterprise environment to protect their own internal assets and provide the full defense-in-depth capabilities from their own environment to their subsidiaries. Providing a highly effective solution that was both easy and fast to deploy, the Attivo Networks® ThreatDefend™ platform gave the most effective return on investment in a complex M&A situation.

ABOUT ATTIVO NETWORKS

Attivo Networks® provides real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, IoT, and other specialized attack surfaces by deceiving an attacker into revealing themselves. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. The company has won over 50 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.