RAPID7

CASE STUDY

Buyer's Remorse No More: Rapid7 Managed Detection and Response Proves Value Through Expertise, Visibility

INDUSTRY:
Finance

SERVICES:
Managed Detection and Response (MDR)

It's no secret finance companies have a lot at stake—they handle incredibly sensitive information for both individuals and organizations alike. For the VP of IT at this finance company, his job was to solve operational problems with technical solutions. He also needed to be able to reassure customers that his organization was doing everything it could to keep their data safe. "Our clients trust us, so we have to make sure we have that trust inside that we can present back to them. We never want to take that trust for granted," he said.

It was paramount that the technical solutions he used and the vendors he worked with provided value whenever he needed to rely on them, especially after an unfortunate security event blind-sided his team in June 2016.

"Since we are a finance company, we have remittance information that comes in. Our clients' customers send us money, and we'll send our clients money." During this security event, before working with Rapid7, the VP explains they were using Office 365, and a user's account got hacked. The perpetrator logged into the account and set up multiple rules.

AT A GLANCE

Network visibility, before and after Rapid7:

BEFORE RAPID7 >

The VP had a vendor conduct a penetration test. He signed the quote, but after a few weeks nothing had been scheduled and he wasn't sure what was going on. A few days later, he received a report from the vendor — without knowing they even ran a test. "That was so scary to me that these guys were on my network and I had no clue," he said.

AFTER RAPID7 >

The VP arranged for another pen test without telling anyone it was happening. He wanted to compare the process. "This was the first true test," he said. "The MDR team knew I was going to run a test, but not when. The test kicked off at 4:02, and by 4:03 I had an email alert already. It was so fast that when I called the vendor to ask if they'd started, the person I was dealing with didn't even know his tech had kicked it off yet."

> “Sometimes you purchase something and get buyer’s remorse. You wonder if you made the right decision. When we were doing the installation, though, that’s when I thought **‘Wow, these guys know their software.’ They knew a fix immediately, for everything.”**
>
> — VP of IT, Finance company

In this instance, he believes the attacker found a user account through lateral movement, set up rules in the account, and then emailed customers to change remittance information from the finance company’s bank to the attacker’s bank. The attacker also set up the rules so that when the emails would go out and come in, they would automatically get deleted. “They did it across tons of different accounts,” he said. “We discovered something was going on when money stopped coming in. Then we went on a spree of finding fixes.”

He purchased Office 365 licenses for visibility into the network, but found that they didn’t offer insight until 24 hours later. Once he did start getting more visibility, he saw there were four additional users logging in from Nigeria, when the user accounts were associated with a city in Texas. “At that moment, I realized that I needed something.”

When You Need More Than Vulnerability Management and Pen Testing

At first, the VP downloaded Rapid7 Metasploit, the world’s most used penetration testing framework, and Nexpose, Rapid7’s leading vulnerability management product, to manage the organization’s environment himself. However, he quickly realized that he needed more visibility. He pivoted to start looking for robust incident detection and response service solutions that offered a layer of service on top of a product, including one vendor owned by a computer manufacturer. But the more he looked into it, the more he found that the vendor’s statements didn’t hold up against the testing/POC, that hardware wasn’t included in the service, and that they didn’t offer much transparency. Not to mention, it was expensive compared to the quote Rapid7 provided him for their services. Rapid7’s Managed Detection and Response (MDR) team offered hunting and partnering out of a security operations center (SOC) in Alexandria, VA. The team is dedicated to keeping customer organizations safe with expertise in user behavior analytics, attacker behavior analytics, threat detection, and more.

The VP was already familiar with Rapid7 through Nexpose and Metasploit, and he knew their products worked. Add the fact that he found Rapid7 to have a strong reputation in the market and that the Managed Detection and Response team offered prevention efforts, and the VP had a simple response: “Why wouldn’t I go with Rapid7?”

The “Service” Side of Managed Services

The VP worked with Rapid7’s MDR team to set up the baseline, after which he says the process was simple, which is pretty remarkable considering the complexity of what Rapid7 does. Not long after, he saw the team’s expertise firsthand.

“Mike [Scutt] and David [O’Hara] knew everything. Every little tidbit, they just knew,” he said. “Sometimes you purchase something and get buyer’s remorse. You wonder if you made the right decision. When we were doing the installation, though, that’s when I thought ‘Wow, these guys know their software.’ They knew a fix immediately, for everything.”

Once the service was up and running, the VP immediately started receiving alerts from Rapid7. As a finance company, they had valid authentications coming in from multiple locations, so he was looking for a way to authenticate those and be alerted to any brute-force attempts. Two scenarios highlight what the Rapid7 team was able to offer:

- **Scenario 1:** The VP received an alert that a brute-force attack was happening through a management server. He changed the port and thought doing that, plus having a valid login, was good enough. But Rapid7's MDR team caught the login information and the logs, and they were able to tell him which specific IP address range to block, sending a message to the attacker that they were on to him or her.

- **Scenario 2:** The VP received an alert to lateral login movement from a user accessing four other computers within minutes of each other. After receiving the alert, he logged in and noticed some odd network traffic, at which point he discovered the user had downloaded a ransomware virus. The last time the company was hit with a ransomware bug, it cost 14 hours of downtime, not including the three days it took to restore from their backups. This time, however, there was no need to spend time restoring systems because he was able to clear the infection within 12 minutes of receiving the alert from Rapid7.

"Everything I need, Rapid7 covers," the VP said.

Staying in the Know

After the events of June 2016, the VP says "I didn't know" wasn't an acceptable answer when company owners asked how something like that could happen.

"Now I meet with the CEO every week, and he always asks how security is going. Since I've had Rapid7's team in place, it's easy to say 'Everything's good,'" he explains. "And that's not because nothing ever happens—it's the exact opposite. It's because I know whenever something happens."

"I don't kid that I sleep better having Rapid7 in place. Before it was the fear of what could be going on that I don't know about," he continues. "You never know what's happening on your network until you get something like Rapid7. It's just amazing to me."

"You never know what's happening on your network until you get something like Rapid7. It's just amazing to me."

— VP of IT, Finance company