The Case of the (Missing) Unpatched Environment

Overview

- A national retail franchise sought cyber coverage from Corvus after an exorbitant renewal premium quoted by their current carrier.
- The Corvus Scan found servers on the applicant's system that had not been patched against the Microsoft Exchange Server vulnerability, despite the applicant and their managed service provider (MSP) expressing confidence that the system had been patched.
- The Corvus team dug into the results and located the specific issue, uncovering a chain of miscommunication between the MSP and client that had led to the gap in security.
- With the system patched, Corvus was able to produce a competitive quote and bound the account.

During this difficult time in the market, it is imperative to have a team like Corvus who is willing to take the time to help the insured dig into not only their system — but also the vulnerabilities brought by their vendors.
Broker Ashley Ganne, AVP at Brown & Riding

The Situation

In March 2021 wholesale broker Ashley Ganne, AVP at Brown & Riding, sought a quote for a large national retail franchise who was facing a challenge familiar to many organizations: a hard market for Cyber insurance. The incumbent carrier had increased premium on the renewal to a level the client felt was exorbitant, despite the fact that the account had remained loss-free for several years.

Here's how Corvus addressed the risk and ended up with a safer policyholder (and a happy broker).

The Challenge: Critical vulnerability, or false positive?

As part of our quoting process, we examine the organization's IT footprint with our proprietary scan technology, the Corvus Scan. It's a non-invasive approach for us to understand their cybersecurity hygiene and insurance risk. Through a number of techniques, we can identify an organization's IT assets and potential vulnerabilities.

Once we've gathered that information, we're able to share actionable information — sometimes identifying critical vulnerabilities — for the applicant to improve security.

In this case, our scan found issues that the applicant was confident they'd taken care of prior. This resulted in a higher quoted premium than anticipated, as well as some concern. Why was our scan finding vulnerabilities, including unpatched Microsoft Exchange software, that the client thought they had already addressed?

The mass exploitation of Microsoft's on-premise Exchange Server software in March 2021 was one of the most widespread zero-days seen in years, opening the door to potential threat actors with thousands of unpatched systems left exposed. (Since the day they were released Corvus has focused on making sure our policyholders are up-to-date with updates issued by Microsoft). The client was aware of the Microsoft situation, but believed they had already worked with their managed service provider to address the risk.

The client was aware of the Microsoft situation, but believed they had already worked with their managed service provider to address the risk.

The Solution: Communication and collaboration

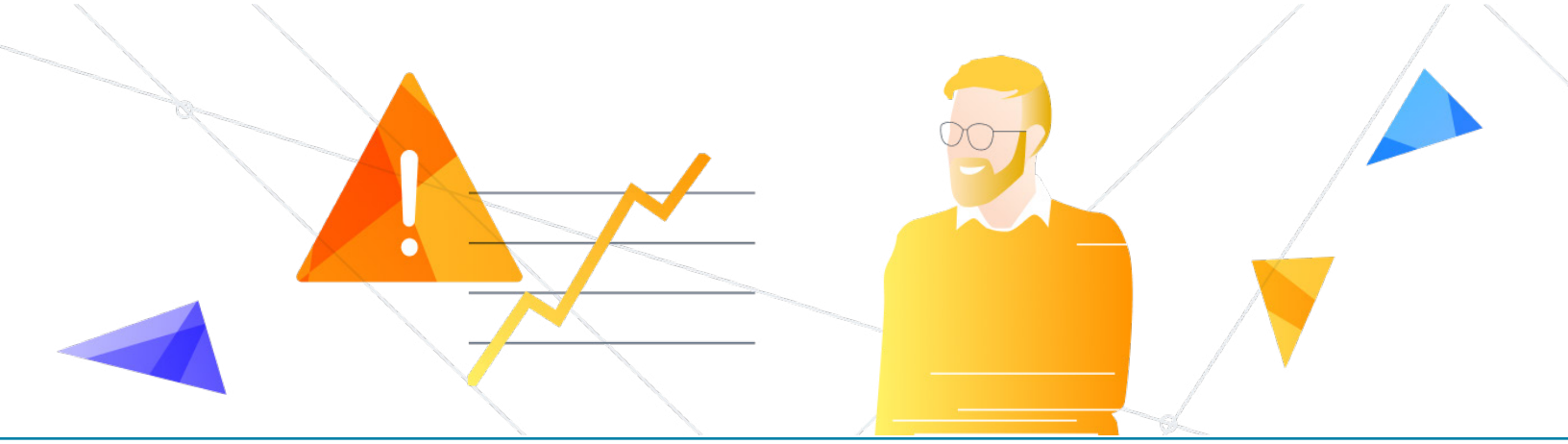
The score our Corvus Scan returned for the client was lower than expected. While the client believed that they had patched their server against the Microsoft Exchange vulnerability, multiple runs of the Corvus Scan were bringing back inconclusive results: sometimes coming back showing the system patched, other times locating IP addresses with the older software version. This called for some conversations between the applicant and Corvus — with both our CISO and VP of Cyber Underwriting discussing the scan in detail — but the client and their managed service provider (MSP) held firm that they had taken care of all of the patching.

Bring on the deep dive. Our Data Science team got to work, digging into the scans and the IP addresses associated with the triggered items. This allowed them to return to the MSP having pinpointed the exact issues, as well as where they were present. The culprit? An initial misstep on the vendor's part that was compounded by miscommunication.

The Corvus team determined that traffic to the applicant's web infrastructure (including our scan's requests) was being routed by the client's load balancer, which acts as a sort of traffic cop to divert web requests to different systems to better manage heavy network traffic loads. It became clear that while the MSP had indeed located and patched one server, they did not realize that a load balancer was actively routing traffic to multiple servers. Ultimately, because of further miscommunication, no one with complete knowledge of the system architecture verified that the patch was installed across all possible destinations for web requests.

Once the source of the confusion was uncovered, the client and MSP were easily able to verify that an instance of Microsoft Exchange servers had indeed been missed, and patched it.

Our Data Science team got to work, digging into the scans and the IP addresses associated with the triggered items. This allowed them to return to the MSP having pinpointed the exact issues, as well as where they were present. The culprit? An initial misstep on the vendor's part that was compounded by miscommunication.



The Bottom Line: Less risk, safer world

The client was able to make final updates to their network, allowing Corvus underwriters to move forward with the process and even reduce the premium. The applicant's willingness to get to the bottom of the issue allowed Corvus to not only limit their vulnerabilities, but also meet their need for cyber coverage.

This example shows how data-driven tools can enable a "trust, but verify" ethos for the current cyber market. If not for the Corvus Scan's results, the applicant would have continued to believe they were safe, and the gap in security would have been left for an enterprising threat actor to find and possibly exploit. Unfortunately, a single unpatched server can result in total network compromise: in cybersecurity posture, you're only as safe as your weakest point.

After we were able to find a solution for her client, Ashley Ganne, the wholesale broker, reflected: "during this difficult time in the market, it is imperative to have a team like Corvus who is willing to take the time to help the insured dig into not only their system — but also the vulnerabilities brought by their vendors."

Unfortunately, a single unpatched server can result in total network compromise: in cybersecurity posture, you're only as safe as your weakest point.

The mission behind our work at Corvus, from the initial scan and focus on vulnerabilities, to the troubleshooting conversations, is to manage risk and protect organizations from an intensifying landscape of threat actors. The insured emphasized that they valued relationships over pricing — we listened, and found a resolution that made them safer, and made our underwriters feel confident in placing the risk.