Success Story

From Crisis to Confidence in Only Hours: How Rapid7 Became a Security Sommelier

What would you do if you found out customers were being spammed with malicious emails claiming to come from your organization? It's a nightmare scenario for any IT professional, one that could indicate a data breach with serious reputational and financial implications. The first step in a thorough response is visibility into key systems. But how? It's a challenge Liberty Wines recently faced and overcame, thanks to InsightIDR and Rapid7's speedy response to a serious security alert.

The attack

The cyberattack came in early 2016, when IT manager Tom Brown was on a trip to eastern Europe. Back at headquarters, his staff reported that email had gone into meltdown. Customers were calling in to report that they received emails from Liberty Wines with an unusual attachment, which turned out to be malicious. At the same time, the team was being bombarded by a backscatter of hundreds of thousands of non-delivery receipts related to the malicious email. Tom had to ensure that this wasn't from an internal breach — that's when Brown called in the experts at Rapid7.

Liberty Wines is a small but globally dispersed, multi-award winning wine business headquartered in London. As IT manager, Brown has to look after 130 endpoints — a mix of desktops, smartphones, and laptops, as well as hosted email and a handful of on-premise servers. With a globe-trotting sales team logging on to the network from around the world, and a diverse IT estate, there's plenty to keep him busy.

Brown had used Rapid7 software in the past and knew of them as a leader in the security space. He had previously identified a need to track and analyze user authentications and behavior but couldn't find anything suitable. Until Rapid7 there really wasn't anything on the market that could easily scale from an SME like Liberty Wines right up to a large enterprise deployment. The architecture of the InsightIDR system allows it to fit any size, both from a scale and a startup cost perspective. He'd arranged for a live demo, been impressed, and allocated budget to install it the next financial year. However, the attackers had other plans.

Down to business

With time now of the essence, Brown quickly purchased and installed InsightIDR to gain the visibility and tools he needed to deal with the crisis at hand. InsightIDR is an integrated detection and investigation solution that combines user behavior analytics, endpoint detection, and visual log search to spot and contain a compromise quickly and effectively. The Rapid7 team worked closely with Brown, across three different time zones, to resolve the issue. Thanks to

LIBERTY WINES

Industry: Wholesale Supplier

Company Size: 100

Products: Nexpose, InsightIDR

"InsightIDR is a great system. It gives you that warm feeling inside by catching any suspicious behavior on the network months before you'd otherwise discover it."

"It makes you think differently about things. IT is always being pulled in different directions, but Nexpose and InsightIDR have given me the tools to say to the customer 'you can't have it this way because it's not secure.'"

Rapid7's Quick Start service, the product began collecting and baselining behavior "almost straightaway" to provide Liberty Wines with the real-time intelligence needed to reliably identify compromise.

It scoured their systems looking for traversal, privilege escalation, unusual service account usage, logins from unexpected locations or devices, and so on. Fortunately for Brown, there was no sign of such activity. Instead, it was deduced that the malicious activity had originated from a customer. The hackers had cloned a genuine email sent from Liberty Wines to a customer and then mass emailed it out to millions of internet users with the addition of a malicious JavaScript attachment.

The Rapid7 team reverse engineered and analyzed the malware in question to ensure that Liberty Wines was not compromised. Combined with the real-time visibility provided by InsightIDR, Brown was able to draw up a clear and detailed graphical timeline of events for the Liberty Wines board, and inform customers on the exact situation. Rapid7's leading vulnerability management solution, Nexpose, was also set to work to identify any potential security weaknesses in the Liberty Wines IT setup.

A lasting confidence

Brown was delighted by the speed and accuracy of the incident response investigation. Rapid7 was able to integrate InsightIDR into the Liberty Wines environment within hours. That speed of response is essential in suspected breach incidents, as the longer an attacker is allowed inside a system, the greater the financial and related damage likely inflicted.

"InsightIDR is a great system. It gives you that warm feeling inside by catching any suspicious behavior on the network months before you'd otherwise discover it," says Brown. "Most IT managers accept that something will get through, that there will be a hole somewhere. So it's about finding out where it is quickly and being able to take action, and that's what InsightIDR gives you. It's also helped me better manage our users from day to day."

Although there was no sign of a breach, the new user and endpoint process visibility it gave Liberty Wines did highlight a few areas they needed to tighten up, particularly on user account security. The whole process of managing Liberty Wines staff is now more efficient and secure thanks to the highly granular visibility InsightIDR provides. It enables Brown to see if a user is trying to access work emails on an unsanctioned mobile device, for example, or if they're logging on from a foreign country. In combination with Nexpose, Rapid7's vulnerability management product, it has helped him become a more effective IT manager, he says.

"It makes you think differently about things. IT is always being pulled in different directions, but Nexpose and InsightIDR have given me the tools to say to the customer 'you can't have it this way because it's not secure.'"

In fact, thanks to running Nexpose, Brown was able to first quantify and then demonstrate to the business how legacy non-production servers, which were left running for reference purposes, presented a major security risk if left operational. As a result, he got the backing of senior management to completely shut down the firm's legacy servers to lock down this risk for good.

With these kinds of results, it's no surprise Brown is keen on expanding Liberty Wines' relationship with Rapid7. With a new website on the way, he's already set aside budget for a pen testing service to make sure the site is "bomb-proof" when it goes live. And he's scoping further future investments into Rapid7 Security Awareness Training services.

The incident may not have turned out to be a breach in the end, but thanks to Rapid7's comprehensive response, Liberty Wines is now able to manage its staff and secure its IT estate in a more effective, proactive manner. That's something we can all raise a glass to.