FORCEPOINT
POWERED BY Raytheon

Case Study

Forcepoint: Securing Data During an M&A

"Having the Forcepoint DLP solution running in our environment allowed us to successfully protect our data, while preventing any form of data leakage during our M&A."

— Dave Barton, Chief Information Security Officer, Forcepoint

INDUSTRY
Cybersecurity

COUNTRY
United States

PRODUCT TYPE
Forcepoint DLP
Forcepoint Insider Threat
Forcepoint NGFW

SIZE
2,500 Users

SECURITY ISSUE
Securing Data During an M&A

OVERVIEW

On January 14, 2016, a new joint venture built on the integration of Websense, Raytheon Cyber Products (RCP), and the Forcepoint NGFW business was announced. Known as Forcepoint, this new company is the culmination of nearly a year's worth of business systems integration.

Dave Barton, Chief Security Officer at Forcepoint, was pivotal in making sure that forward progression through the M&A process focused on protecting employees, data, and IP.

CHALLENGE

The problem most companies face while going through M&A activities, Barton says, is a lack of due diligence in the security phase. The majority of businesses will not think twice about where its sensitive data is located, how it is being protected, or how an acquisition might impact the exposure of its IP.

Proper security due diligence confirms that the policies in place are actually in practice and highlights potential disparities. For instance, one organization could have more strict security requirements, requiring the other organization(s) to be brought into alignment. In addition, employees of companies going through M&A activities typically have some level of angst because of what they think it might mean for them – up to and including losing their jobs. When people begin to question job security, they tend to deviate from their normal behavior, which can increase risk to data. Having the necessary visibility during the M&A process is paramount to protecting critical data.

Blending companies will increase the complexity in protecting an organization's sensitive data. This means that making data accessible to the appropriate parties while simultaneously protecting it from loss, theft, and misuse is essential. A loss of IP or other data has an immediate effect on reputation, can result in legal and regulatory action, and can adversely affect competitive positioning and shareholder value.

SOLUTION

Before any data, systems, or process integration of Websense and RCP, an evaluation of each company's internal and external security posture was necessary. A third-party performed penetration testing and dug into the dark web for any chatter around vulnerabilities or ongoing hacks of which the companies may not have been aware. Security staff members were asked to detail their security programs – including user education, vulnerability management, data classification and flow, and administration of access controls.

First and foremost, Barton and his team focused on 'user awareness' training, a process, Barton recalls, which was crucial to alerting both Websense and Raytheon users that they were going to see targeted phishing campaigns during the M&A process.

As Barton developed user awareness internally, he and his team implemented DLP tools to begin discovering and monitoring critical data. The average organization, according to Barton, doesn't have a handle on where its data sits:

"Fundamentally, they don't even know what their data is classified as. Is it sensitive? Is it restrictive? Is it proprietary? Having knowledge of your data upfront and knowing where it sits allows you to put controls in place to monitor it as you go through an M&A – if I don't know where it, I can't protect it."

— Barton

RCP and Websense's IP, financial data, etc., were identified and the appropriate communications were developed to combat targeted threats and malicious activity (e.g. spam and phishing attacks) which are so common when companies consolidate.

RESULTS

Targeted data theft attempts were aimed at Forcepoint executives by sending seemingly legitimate emails from Raytheon Corporate requesting sensitive data and financial information. Thanks to the proactive measures already put in place, they did not fall victim to these attempted malicious intrusions.

> "The morning we announced the merger at RSA, almost immediately we saw phishing campaigns that looked like they were coming from Raytheon Corporate, but weren't. Our own products protected us and helped to make sure that those emails did not get delivered to our end users."
>
> — Barton

Merging companies is rarely if ever a simple process and the Forcepoint integration was more complex than most. At the same time the Websense and RCP joint venture was being completed, Forcepoint acquired Stonesoft, which required applying the same data protection processes to ensure a smooth and secure integration. In addition, the shift to a new brand identity required unwavering user awareness and an IT team equipped to continuously monitor user behavior.

> "Having the Forcepoint DLP solution running in our environment allowed us to successfully protect our data, while preventing any form of data leakage during our M&A."
>
> — Barton

A successful M&A was ultimately achieved by deploying DLP security tools that restricted the ability to share data containing the new name and other brand information outside of the internal network.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[CASESTUDY_FORCEPOINT_EN] 300078.030117