CASE STUDY

Helping a healthcare leader recover from a malware attack

A major healthcare sector organization struggled to manage in the wake of a malware attack—they needed a knowledgeable expert to help communicate to customers, regulators, and their executive stakeholders, in addition to improving their future cyber posture. A Unit 42 vCISO was on the scene to assist.

paloalto NETWORKS

IN BRIEF

Customer

The client has requested to remain anonymous due to the sensitive nature of the incident

Industry

Healthcare

Products and Services

Unit 42 Virtual CISO (vCISO)

Country

United States of America

Challenges

The organization needed to recover from malware attack, coordinate its cybersecurity response, communicate with customers, legal, and regulators, and define and build a cybersecurity program to ensure it would not happen again.

Requirements

+ Manage malware attack response, communicate with customers, lawyers, and regulators
+ Build a cybersecurity strategy and reduce cyber risks moving forward

Solution

Unit 42 provided a vCISO to manage the breach response, manage communications, and coordinate with internal teams to create a cybersecurity strategy to answer questions about the company's security posture.

CHALLENGE

Navigating a complex and mission-critical response

A national healthcare provider experienced a malware attack that crippled its ability to provide critical business services to its clients. Due to the nature of the attack, executives needed to spend considerable time answering legal and regulatory questions and offering assurances to customers regarding their response to the incident. Without a chief security information officer to oversee the cybersecurity program, they needed a knowledgeable expert to help them communicate with customers, regulators, and executive stakeholders.

REQUIREMENTS

Expert risk management and (stakeholder) communication

The organization determined that they needed a Unit 42 vCISO—a virtual chief information security officer—to help identify and manage risk and interface with customers and regulators to provide updates on the corporate response.

In addition, the client wanted to build a detailed cybersecurity program to improve their security posture, response playbooks, and minimize the impact of future events. Knowing it would take a good amount of time to identify, recruit, and onboard an executive, the organization needed an interim cybersecurity consultant to act in the capacity of a CISO.

SOLUTION

A vCISO helps the organization take charge

Managing highly visible malware incidents can challenge any organization. Many healthcare organizations lack highly expert senior-level cybersecurity staff, making the task even more considerable. In the wake of a malware incident, this organization turned to Unit 42 to serve as a vCISO to identify and manage risk as well as provide extensive communication assistance to customers, attorneys, and regulators, giving status updates on remediation measures implemented to mitigate risk.

The vCISO immediately took charge of the organization's internal cybersecurity team, performing the role of the chief information security officer. The new vCISO was responsible for collaborating with internal business groups to develop a robust information security program, authored a multiyear cybersecurity roadmap of tactical initiatives, and built a short- and long-term budget to support these initiatives.

During the engagement, the vCISO became a trusted advisor to the corporate executives and, ultimately, the board of directors, providing a highly effective communication function internally, externally, and up the chain of command.

RESULTS

Establishing a stronger security posture

With a Unit 42 vCISO onboard, the corporate executives were able to focus on restoring normal business operations while entrusting the vCISO with critical communications functions for customers, attorneys, regulators, and executive stakeholders. The Unit 42 vCISO helped the organization to develop a more robust information security program with the goal of improving its defenses now and in the future.

To learn more about Unit 42, visit paloaltonetworks.com/unit42.

Get in touch

If you'd like to learn more about how Unit 42 can help your organization defend against and respond to severe cyberthreats, visit start.paloaltonetworks.com/contact-unit42 to connect with a team member.

Under attack?

If you think you may have been breached or have an urgent matter, please email unit42-investigations@paloaltonetworks.com or call US Toll-Free: 1.866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, and JAPAC: +65.6983.8730

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.
parent_cs_national-healthcare-provider_092921