2021

CASE STUDY

Improving the Security Posture of a Pharmaceutical Company

Infopercept

Introduction:

A *leading Japanese pharmaceutical giant* is dedicated to creating products for better medical care world-wide. It is a research oriented company that has made significant breakthroughs in the field of science through a number of clinical trials. It believes in cultivating a culture of empathy and creativity. Due to its critical line of work, the CISO of the company takes meticulous steps to secure the company's network, infrastructure and data.

Cyber security entails *regular checks and maintenance*. It also requires random testing to ensure that there are no loopholes in the network. In order to improve the security posture of the network and to check whether the external and internal applications are safe from hacks; the organization hired ***Infopercept, a global managed security services provider.***

Infopercept, a recognized name in the field of cyber security, is known for its diligent efforts in providing *customized solutions* based on the requirement of the clients. It does an in-depth assessment of security before arriving at a strategy.

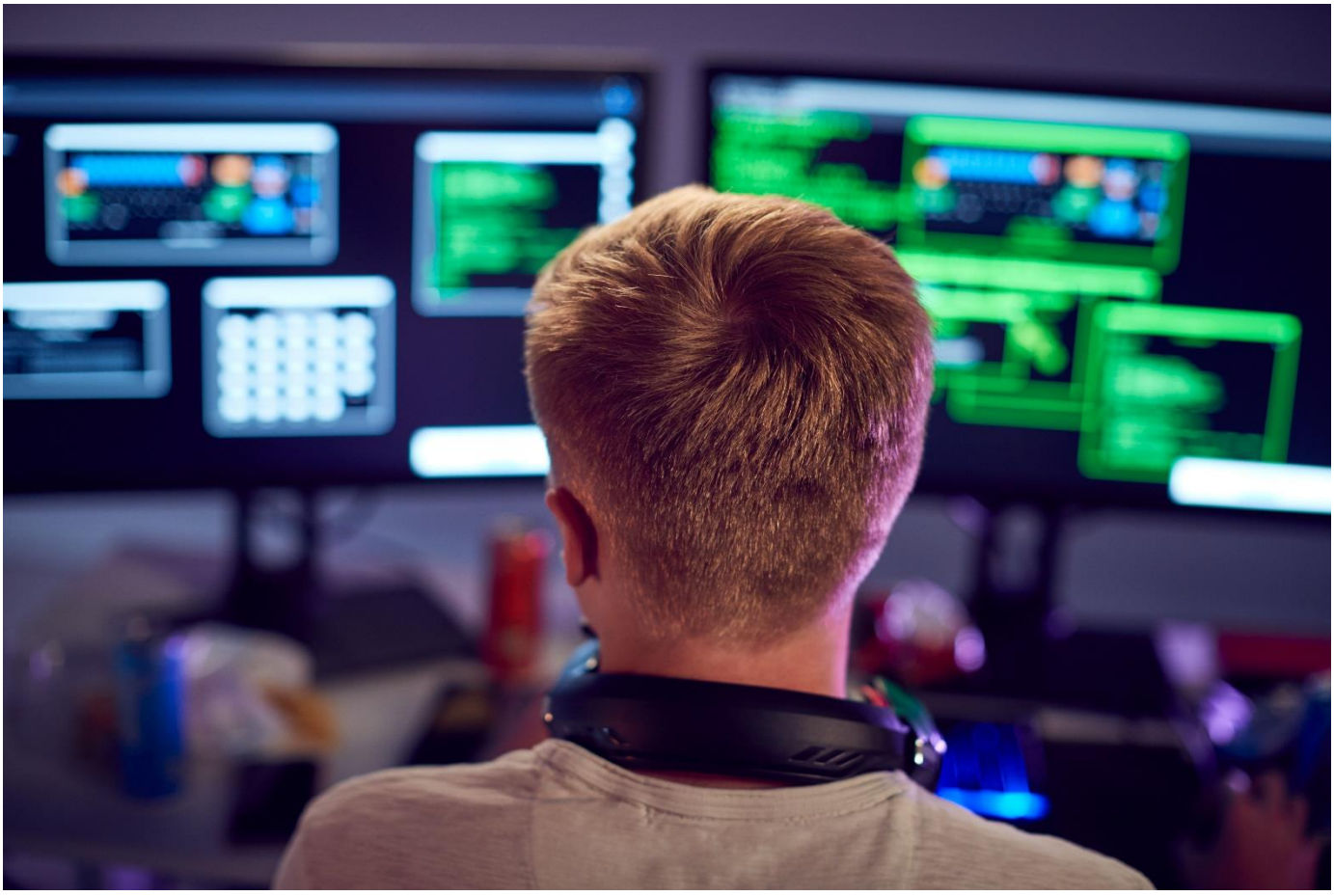
In the case of the pharmaceutical company, Infopercept was well aware of the serious nature of the data. A vast amount of sensitive data such as those pertaining to clinical trials, or formulae of new medicines, vaccines etc. are stored on the network. Considering that a lot of confidential data is at stake, Infopercept took extreme care and precaution while evaluating the systems network.

Infopercept sent across a **Red Team** to scrutinize the network. The IT professionals who constituted the team *simulated the actions of their real-life adversaries* in order to identify the vulnerabilities and test their ability to detect and respond to real-life threats. Infopercept further did a complete review of the application source code to check for anomalies.

Phishing exercise was also taken up as part of the scrutiny. A number of malicious emails were sent to the staff to gauge their responses to phishing attacks.

The Problem

The team was able to identify a number of vulnerable areas which required immediate remediation. A *number of loopholes* were found in the internal as well as external applications. They were able to *break through the admin privileges* with ease and were able to gain access to their data systems. The *password file was not encrypted* either leaving the entire system exposed. In no time, the Red Team was able to penetrate into their core area of work and research.



Solutions:

Infopercept came up with a variety of solutions to beef up the network security. It launched an **Offensive Strategy** as a part of its **Offensive Security Practices; a proactive approach that uses the latest cybersecurity tactics and techniques.**

Vulnerability Assessment and Penetration Testing (VAPT)

Continuous VAPT – Vulnerability Assessment and Penetration Testing was done, which involves vulnerability scanning to help classify security risks and provides services to mitigate them.

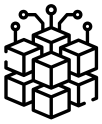
Application Security

Application Security was done to fix vulnerabilities at the application level in hardware and software processes. It is often indicated that a majority of security violations happen at this level. Thus they have to be dealt with early on, to prevent them from becoming serious security breaches.

DevSecOps

DevSecOps is the emerging mindset that ensures IT teams work in collaboration with the developers to produce the desired security results.

Breach and Attack Simulation (BAS)



The BAS system, as it is popularly known as, is a relatively new technology that not just identifies vulnerabilities in a system but goes a step ahead and recommends and prioritizes the solutions.

Continuous Automated Red Teaming (CART)

CART, although automated, is an intense effort to identify vulnerabilities and exposures It helps prevent future breaches and analyzes security defenses in the real-world.

A debriefing was done with the CISO and the IT team appraising them of the measures taken and the strategies that need to be undertaken in the future to ensure the complete protection of their network security.

About INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint

Publisher
H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info
M: +91 9898857117
W: www.infopercept.com
E : sos@infopercept.com

Global Offices

UNITED STATES OF AMERICA
+1 516 713 5040

UNITED KINGDOM
+44 2035002056

SRI LANKA
+94 702 958 909

KUWAIT
+965 6099 1177

INDIA
+91 9898857117

Infopercept