HealthManagement
Promoting Management and Leadership

SANS-Norse Report: Cyberattacks Compromising Healthcare Organisations

Norse Global Threat Intelligence Platform Identifies Healthcare Organizations' Compromised Networks, Applications, Devices and Systems

In association with SANS, the most trusted and largest source for information security training, certification and research, Norse, the leading provider of live threat intelligence solutions, has released the SANS-Norse Healthcare Cyberthreat Report.

Developed by Senior SANS Analyst and Healthcare Specialist Barbara Filkins with intelligence gathered by the Norse global threat intelligence platform, this report reveals that the networks and Internet-connected devices of organisations in virtually every healthcare category, ranging from hospitals over insurance carriers to pharmaceutical companies, have been and continue to be compromised by successful attacks.

Frequently leading to a data breach, a network compromise can potentially expose the personally identifiable information of millions of consumers, as well as the organisation's own intellectual property and billing systems. This enables cybercriminals to use the organisation's network infrastructure and devices to launch organised attacks on other networks, and to execute billions of dollars worth of fraudulent transactions.

Some of the most alarming findings uncovered during the intelligence-gathering period include:

As a small sample, close to 50,000 unique events of a malicious nature took place within the healthcare IT environment
Networks and devices at more than 370 US-based healthcare-related organisations were compromised, and some of them are still compromised.
Compromised devices included radiology imaging software, web cameras, firewalls and mail servers.
A significant number of compromises were a consequence of very basic issues such as not changing default credentials on firewalls.

Filkins explained how this level of compromise and control could easily lead to a wide range of criminal activities that are currently not being detected. She cited the example that hackers could engage in widespread theft of patient information including everything from medical conditions to social security numbers to home addresses, even the manipulation of medical devices used to administer critical care. Filkins went on to state that for many organisations governed by stringent regulations such as the Healthcare Insurance Portability and Accountability Act (HIPAA), compromises and breaches lead to massive fines. In 2013, fines ranged from $150,000 and went up to $1.7 million in the widely publicised WellPoint case.

Larry Ponemon, Chairman of the Ponemon Institute, emphasised the magnitude of importance which cybersecurity holds for healthcare IT. According to him, current HIPAA and HITECH compliance does not provide nearly enough security, and with healthcare organisations falling further and further behind in their efforts to secure patient data, Ponemon stresses that the security of healthcare data must become the priority for healthcare organisations. Since a large percentage of medical institutions have been victims of cyberattacks which have caused millions and billions of costs, the chairman believes the report helps sound a very necessary alarm.

The SANS-Norse Healthcare Cyberthreat Report can be found online .

Source: Norse

25 February 2014

Published on : Tue, 25 Feb 2014