REDSOCKS
malicious threat detection

Breach Detection in Healthcare

How to keep sensitive data safe within Healthcare organizations.

Healthcare organizations such as hospitals and clinics are facing new and unique challenges. Cybercriminals are nowadays actively targeting the healthcare industry.

Digital records of patients have become part of our daily reality. In hospitals, doctors' offices, insurance companies, and other related organizations, many people need access to patient records to do their jobs. However, how do we know someone else cannot gain unauthorized access to these files?

Protecting those files is vital and a lot of attention, effort and technology is put into it.

Challenge 1: Security awareness is not in the DNA

Healthcare organizations are more susceptible to these attacks as they are usually behind other industries in respect to information security. The healthcare industry only recently went through a massive transition with regard to technology and is now facing threats that never existed before. Healthcare organizations now need to educate themselves about the threat landscape and build a new strategy that adopts several cybersecurity strategies from other industries.

Challenge 2: Medical Equipment issues

Organizations which have specialized medical devices are using newer technologies such as wireless capabilities. Hence, they have a greater level of susceptibility to various information security risks.

According to Deloitte's Networked medical device cybersecurity and patient safety report, medical devices are closed systems, that cannot be easily scanned for malware. Devices, including MRI scanners, x-ray machines and drug infusion pumps, are vulnerable to hacking, creating significant health risks for patients.

RedSocks Benefits

- √ **Turn-key solution**
- √ **Compliant with Eu GDPR and NL Mandatory Data Breach Notification Regulation**
- √ **No extra burden on your administrator**
- √ **Preserving your security and privacy**
- √ **No impact on stability & performance**

Three examples of threats according to the report:

- Unauthorized access: for example, a malicious person intercepting and altering signals sent wirelessly to the medical device
- Malware: a malicious software program designed to carry out annoying or harmful actions and often masquerading as or embedded in useful programs so that users are induced to activate it
- Denial-of-service attack: computer worms or viruses that overwhelm a device by excessive communication attempts, making the device unusable by either slowing or blocking functionality or draining the device's battery.

Challenge 3: Compliance and regulation

With data breaches in healthcare expected to rise, government regulations, such as EU GDPR and the Dutch Mandatory Breach Notification act, are imposing

regulations that are broader in reach than ever before. Today's penalties for data breaches increase, notification requirements are more stringent, and enforcement agencies have new incentives for taking action against organizations that fail to protect healthcare privacy. Next to that, the requirement to publicly notify customers about the data breach means lost trust and tarnished reputations for brands, which negatively impacts the business' bottom line.

Challenge 4. Not having dedicated full-time employees in charge of data

Traditionally, data security has been regarded by the C-level managers as a burden - an expense with no direct revenue stream. As a result, many hospitals do not even have a single dedicated full-time employee in charge of data. However, having a trusted employee like a security officer or a CISO is crucial, as data security breaches demands significant expertise, both technical and organizational and often require timely action.

How to Strengthen Healthcare Security?

A new approach has to be deployed, including layered information security products deployed with custom configurations. Additionally, a more proactive model, where organizations have real-time situational awareness or insights into emerging cyber threats, has to be implemented.

Using a point solution like RedSocks Malicious Threat Detection (MTD) breach detection as a "first line of defense", which is designed with rapid implementation and low maintenance in mind can easily solve many of the challenges described above. One of the big advantages of using the RedSocks solution is that you don't need intimate knowledge on configuring and running threat detection on your network. RedSocks invests significant time, resources and expertise making sure its solutions are always using the most up-to-date assessment algorithms and the latest available threat intelligence. RedSocks facilitates management and response , the administrative burden is minimized and the organization can respond when a threat is detected.

Improving Security and Meeting Compliance Needs with RedSocks

The RedSocks Maliciuos Threat Detection (MTD) solution can help healthcare organizations both increase their security posture and address requirements of the GDPR regulations.

To ensure that data breaches are always detected at lightning speed RedSocks provides a critical cyber security layer inside the network perimeter. The solution detects malicious activities and registers data breaches in the technical information infrastructure. It enables your organization to:

- Take action and simplify data breach reporting;
- Put in place a data breach notification procedure;
- Create compliance statements for annual business reports;
- Set up and undertake regular compliance audits;
- Store your data forensically sound for up to 36 Months

Conclusion

By having a unified view of security-related activity on network devices (IoT), firewalls, servers, desktops and breach detection, RedSocks provides, security operations teams with a much richer and more accurate knowledge base from which to observe, interpret and react to possible threats to the organization.

If you are looking to improve capabilities to detect and analyze Advanced Persistent Threats, Breach Detection and Threat Intelligence you can easily do this with the RedSocks platform. To learn more, contact our team via sales@redsocks.nl

For more information

sales@redsocks.nl

http://redsocks.eu/healthcare

Adres: Laan van Nieuw-Oost Indië 133f, 2593 BM Den Haag, The Netherlands | **Tel:** +31 (0)88 13 33 333 | **Email:** info@redsocks.nl