Revolutionizing healthcare security: moving beyond pentesting

BY INTI DE CEUKELAIRE · MARCH 25, 2024 · LAST UPDATED ON MARCH 6, 2025

The healthcare sector remains a prime target for cybercriminals, with 90% of healthcare institutions experiencing at least one security breach in the last few years. And the fallout can be huge.

In 2023, the average cost of a data breach across all sectors was $4.45 million. However, the average cost of a healthcare data breach was $10.93 million – the highest of all industries.

So why is the healthcare industry so relentlessly targeted?

The healthcare industry: a prime target for cybercriminals

Patient information, medical histories, and billing details are valuable on the dark web. These can then be exploited for several purposes, from identity theft and insurance fraud to ransomware attacks and espionage.

Furthermore, the critical nature of healthcare operations renders them particularly vulnerable to cyberattacks. A ransomware attack or data breach can cripple healthcare facilities, disrupting patient care, compromising medical devices, and, ultimately, jeopardizing lives.

Healthcare organizations are grappling to balance accessibility and security, and cybercriminals waste no time in seizing the opportunity to exploit weaknesses in their defenses.

Where does traditional pentesting fall short?

In response to these escalating cyber threats, many healthcare organizations have turned to traditional pentesting as a cornerstone of their cybersecurity strategy.

Pentesting, characterized by periodic assessments of network vulnerabilities and security controls, provides valuable insights into existing security gaps. However, its reliance on point-in-time assessments leaves healthcare organizations vulnerable to threats that evade detection between evaluations. While a valuable tool in cybersecurity, pentesting alone falls short for the healthcare industry due to several factors:

1. Pentesting is reactive in nature

Traditional pentesting operates within a reactive framework, conducting periodic assessments to identify vulnerabilities at one point in time. However, in the healthcare industry, where new threats emerge daily, this reactive approach leaves organizations vulnerable. Vulnerabilities can go undetected between pentests, and so the healthcare industry requires a more proactive approach to security.

2. The ever-evolving array of threats

Healthcare organizations face a diverse array of cyber threats, ranging from ransomware attacks to data breaches and insider threats. With cybercriminals continuously devising new tactics and exploiting vulnerabilities, traditional pentesting may struggle to keep pace with the evolving threat landscape.

3. The criticality of healthcare data

Patient data is the lifeblood of healthcare organizations, containing highly sensitive information such as PII and medical histories. Any compromise of this data can have severe repercussions, ranging from financial losses and legal liabilities to potentially harming patients' lives. Relying solely on traditional pentesting may leave healthcare institutions inadequately shielded and vulnerable to potential breaches.

Taking all of this into account, it's clear to see that healthcare organizations require a more proactive and comprehensive approach to cybersecurity, such as continuous testing.

Continuous testing in the healthcare industry

Unlike traditional pentesting, which offers an intermittent snapshot of an organization's security posture, continuous testing offers ongoing surveillance and detection of threats in real-time.

By continuously scanning for vulnerabilities, healthcare organizations can stay one step ahead of cyber threats, mitigating risks before they escalate into full-blown breaches.

So, how can healthcare companies adopt a continuous approach to security testing? One popular method is running a bug bounty program.

Bug bounty programs invite ethical hackers from around the globe to identify and report vulnerabilities within the organization's systems and applications. Companies incentivize these ethical hackers, often referred to as researchers, with monetary rewards (bounties), swag, or recognition for their findings.

By leveraging the collective expertise of a diverse pool of security researchers, bug bounty programs enable healthcare companies to continuously identify and remediate vulnerabilities in real-time.

Hybrid pentesting: a modern approach

Another approach for healthcare organizations to consider is hybrid pentesting. Hybrid pentests are a new approach to security testing, combining the best of both worlds from traditional pentests and bug bounty programs.

This means that, just like with traditional pentesting, researchers will conduct their search for security relevant issues with the full attention of a traditional pentest, concluding with a report that highlights key findings.

At the same time, it means that organizations have access to the greatest minds of the wider researcher community. They can also benefit from a 'pay for impact' model, where cost is directly scaled with the impact of the findings (with an upper limit agreed upon). This results in greater cost efficiency than traditional pentests.

A continuous approach to security testing is a must for healthcare organizations

Traditional pentesting alone is no longer sufficient to defend against relentless cyber threats. By adopting proactive defense strategies, healthcare organizations can safeguard patient data, maintain trust, and mitigate cyber threats effectively.

To learn more about bug bounty programs and hybrid pentesting for the healthcare industry, get in touch.