INDUSTRY INSIGHTS

Managing Cyberthreats in the Pharmaceutical Industry

A Conversation with Fortinet Healthcare CISO, Troy Ament

Ransomware is a top-of-mind cybersecurity challenge for the pharmaceutical industry, affecting everything from legacy hardware and software systems to aging operational technology (OT) manufacturing environments. Fortinet Healthcare CISO, Troy Ament, shares insights and recommendations designed to help security professionals fortify their environments as well as mitigate and alleviate cyberthreats.

What are the top cybersecurity threats and challenges that today's pharmaceutical companies need to address?

Troy Ament (TA): Pharmaceutical companies have a few primary challenges and threats that are amplified in their vertical, including aging OT manufacturing environments and the convergence of IT and OT systems, along with network security. It's a fact of life that legacy software and hardware systems that are common in pharmaceutical and manufacturing environments were not created with security in mind.

Other challenges are network and security complexities. A lot of organizations implemented a best-of-breed approach, which caused:

- Lack of end-to-end visibility
- Threat response that couldn't be automated because of integration issues
- Prohibitive compliance demonstration because it is resource intensive
- Efficiency challenges due to managing multiple tools
- Skills and training gaps for managing those tools
- Expanded attack surface because of cloud migrations, connective medicine, endpoint expansion, and telework

Another challenge is insider threats, which are amplified in pharma. At my past organizations, we grew with 25 acquisitions over 10 years. With every acquisition, you have to reset your security program and assess that organization because there is potential to introduce new risks. In pharma, there are a lot of alliances and partnerships, typically more with research and development manufacturing organizations, so organizations must implement a least-privilege configuration strategy.

And lastly, global compliance obligations must be met. Pharma organizations span the globe and must meet new and evolving compliance regulations. Plus, the cybersecurity skills shortage is also a problem in the industry.

What is the best way to measure the effectiveness of our current cybersecurity implementation?

TA: Transparency, governance, and alignment with a security framework are very important. A couple of examples of cybersecurity frameworks to follow are the Health Information Trust Alliance and the National Institute of Standards and Technology (NIST). This is in addition to continually embedding security into digital transformation and governance initiatives. Program assessments using different partners and internal teams, such as internal audits, should also be conducted regularly.

What is the cybersecurity maturity scale? What is the time frame to achieve full maturity?

TA: The NIST Maturity Scale provides organizations with five straightforward levels of maturity. *What is the timeframe* is a question that I often get asked by boards and the C-suite because they want to become as secure as possible as quickly as possible. But the answer is dependent on where the organization starts on the maturity scale and on their strategic goals. For example, any mergers and acquisitions they are involved in could set them back or make it take longer for them to achieve level 5—the highest level of security maturity. But also, there is no finish line because once you think you're at the end, the threats evolve, as does the organization. So, it's a continual journey for each organization.

How should organizations prepare for when (not if) they experience ransomware or a cyberattack?

TA: Embedding security into an organization's culture is super important. Organizations that have a successful cybersecurity culture within their organization make it a team sport. They communicate from the top down and the bottom up. It is everyone's role to ensure the organization continues to be secure. Also, these organizations actively exercise their response tactics via tabletop exercises, which are just as important as exercises for things like natural disasters. So, including all players, whether it's your finance team or public relations team, can set up your organization for success.

What are some next-generation technologies that allow organizations to stay one step ahead?

TA: Organizations that have moved beyond foundational security practices and are making the journey up the NIST cybersecurity framework and maturity scale are focusing more on offense. They are becoming more proactive and utilizing technologies such as digital risk protection services. These services can give you visibility into digital-asset risk and an external real-time view into vulnerabilities not only now but as your organization continues to evolve.

Within digital risk protection services is brand-related risk, providing information on web squatting and proactively providing information and intelligence on credentials that have been leaked via phishing. And lastly, within OT environments and in the connected medical space is deception technology, which can provide decoys, for example. Think about an OT physical device in your environment that is a decoy that adversaries will go after. As we know in healthcare, life sciences, and pharma, those devices are hardcoded in the environment, so if they're sitting on the network and something is contacting them, that's usually because of a set of configurations within the environment. So, when adversaries contact those, they provide high-value alerts to your security operations center teams so that they can respond quickly to adversaries in your environment.

To learn more about Fortinet's cybersecurity solutions for the pharmaceutical industry, visit fortinet.com/pharma.

February 27, 2023 3:47 PM

1971353-0-0-EN