The Final Security Layer: Defending Pharma With Deception Technology

Troy Ament, Fortinet Healthcare CISO

What is the average duration?

Cybercriminals have been on the attack against pharmaceutical companies since they realized that the combination of valuable information and the convergence of OT and IT environments made them a more attainable and attractive target. For example, many large pharma companies were targeted in the last few years as vaccines became top of mind around the world.

And just to add insult to injury, this sector ranks third in breach costs. IBM reported in its 2021 Cost of a Data Breach Report that the average pharma data breach costs $5 million per incident. What's more, Constella Intelligence found that the volume of identity records exposed each year for pharma companies rose from 206,475 in 2018 to over 2.5 million in 2020.

Aside from the financial burden, such attacks can shut down vital operations, which can slow or halt research and production. A sound cybersecurity strategy recommendation includes many options, but deception technology is something that not every organization considers. As part of an overall cybersecurity portfolio it can be a useful weapon to add to strengthen and continuously improve cybersecurity posture.

A Primer On Deception Technology

A company can use deception technology to divert hackers from its genuine assets and lead them to a fake or trap. The decoy mimics authentic servers, apps and data to trick the bad actor into believing they have infiltrated and gained access to the enterprise's most valuable assets when they haven't. Using this technology can lessen damage and protect a business's actual assets.

Even while it's not typically the first cybersecurity tactic used by enterprises, it can be a means to improve current security measures, particularly as criminal reconnaissance grows. Any security strategy should work to prevent all unauthorized access, and deception technology can be a useful technique to have on hand if a breach has been discovered.

Additionally, deception technology can be integrated with other tools that help IT security teams spot trespassers. For example, tracking information could be included in the files of a database of fake credentials. When a file is opened, a notification can be sent to the security operations center. Another technique is to use "sink-hole" servers to divert traffic; this tricks malware and bots into reporting to law enforcement rather than to the cyber-attacker.

How Deception Helps Pharma

With deception technology, pharmaceuticals firms now have the chance to adopt a much more proactive approach to security than they previously had. Since pharma is so often under attack, establishing active defense of this kind is a means to restore control and strengthen the last line of defense against attack.

Setting up employee portal decoys is one way to be proactive. Attackers frequently search a pharma company's website or network for access points. However, in some circumstances, they just search for open IP addresses or ports in an effort to locate particular portals that may be accessible. In this way, they frequently run into a bogus employee portal. Since the company doesn't promote this employee portal to its staff or list it on its website, any time a visitor arrives there, an investigation should be launched.

A team of IT professionals can also determine which assets are most appealing to attackers by using deception technology. For example, while it is reasonable to believe that a database of user data – including Social Security numbers and payment details—is an enticing target, you may verify that these are the actual assets hackers are after by using this technology.

Putting Deception In Motion

Deception technologies must be set up with a thorough grasp of your environment and clarity about your most valuable assets. Automation of deployment is made possible by virtualization, which is the foundation of deception technology. For example, efficient deception technology will automatically generate a network asset inventory. Based on the inventory, the platform will automatically build the deception elements, assess them and deploy them to simulate an environment. Deception technology can also help security teams understand the assets that the company has and how well a deception deployment is safeguarding them.

Contrary to popular belief, deception technology can be especially helpful for smaller companies, which may not have the resources to employ more advanced solutions or engage a full security staff. A deception solution's greater visibility can be helpful for companies of all sizes—not just the big players.

Deceive to secure

The pharma threat surface grows with the convergence of OT and IT, and with the proliferation of employee portals. Pharmaceutical companies can use deception technology to reduce network damage and keep an eye on the tools that bad actors use. It serves as a final layer of defense, further protecting the crucial information that this sector requires to do its life-saving work.

Originally published by Healthcare Business Today on March 31, 2023.

April 26, 2023 9:26 AM

2104250-0-0-EN