WSJ PRO

CYBERSECURITY

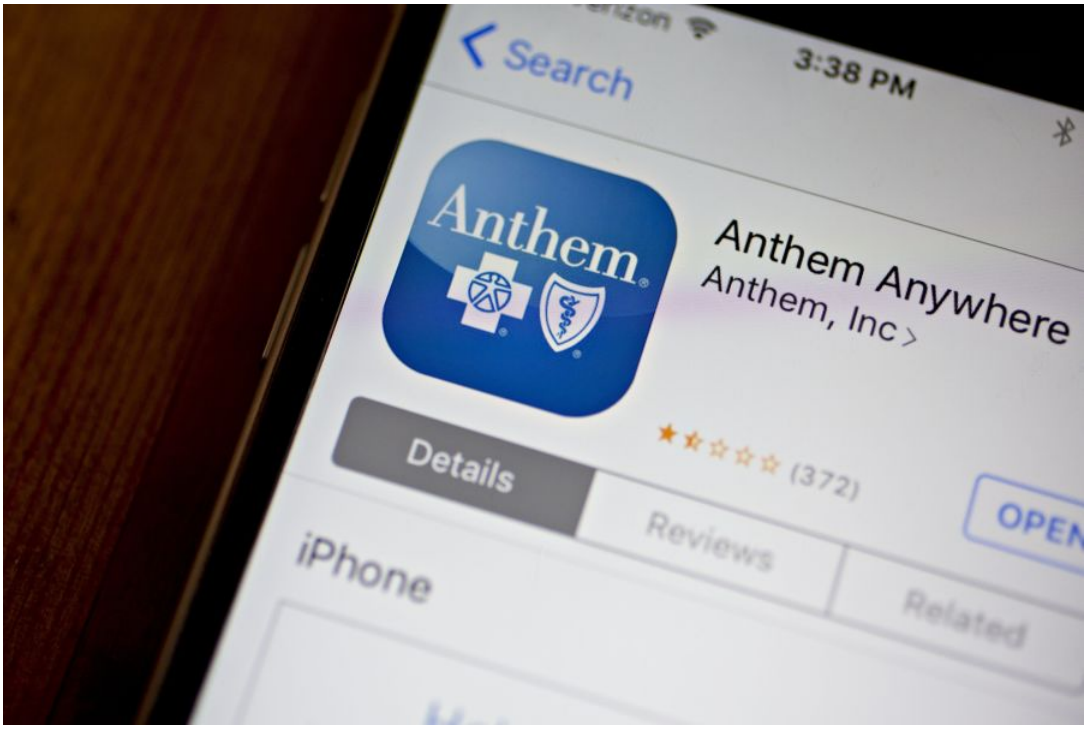
Cyber Daily: Artificial Intelligence in Defense of Patient Data

By Kim S. Nash

Good day. Hackers are going after hospitals to steal valuable personal information, leading security officers in the health-care industry to try clever forms of artificial intelligence to stop attacks. Breaches at healthcare organizations cost an average of $408 per compromised record--by far the highest of any sector, reports WSJ Pro Cybersecurity's Adam Janofsky. To combat the threat, **Wellforce**, a network of Massachusetts hospitals, uses AI to help dangle data on its network to entice hackers, then watches what intruders do. The game helps Wellforce understand hacker behavior and formulate defensive strategies.

Did you receive this newsletter from a colleague? Subscribe yourself here.

Hospitals Turn to AI to Spot Suspicious Behavior and Uncover Hackers



Anthem Inc. in 2017 agreed to pay $115 million to settle a lawsuit over a 2015 cyberattack that exposed the data of more than 78 million people. Here, the Anthem Anywhere application is seen on an Apple Inc. iPhone in Washington on April 21. PHOTO: ANDREW HARRER/BLOOMBERG NEWS

By Adam Janofsky

Healthcare organizations, which suffer breaches that are on average twice as expensive as those in any other industry, are turning to artificial intelligence to help spot malware and stop hackers.

Hospitals in recent years have seen a spike in the amount of patient data available to them, due in large part to the adoption of connected medical devices that gather and transmit patient information in real time. An average hospital bed has more than 15 devices connected to it, and large hospitals typically have about 15,000 connected medical devices on their network, according to Jonathan Nguyen-Duy, vice president of strategy and analytics at cybersecurity firm **Fortinet Inc.**

This influx of data can be dangerous in the hands of hackers. Some hospitals are defending themselves with AI, which can analyze vast amounts of information and detect anomalies faster than humans can. Security teams are using AI in traditional malware and intrusion detection tools to spot anomalies, as well as in experimental methods to deceive hackers.

“Most of the equipment we bring into our medical center to treat patients has a digital component to it,” said Taylor Lehmann, chief information

security officer at **Wellforce**, a 12,000-employee health system that includes Tufts Medical Center and several other Massachusetts hospitals.

Identifying Intruders Faster

Wellforce uses AI to scan for malware that may not be detected by traditional security tools, which work by comparing malware signatures to ones that have already been identified in a database.

"Attackers are using exploits and methods that we've never seen before, and that's where AI can help," Mr. Lehmann said. "There are scenarios where we've never seen a certain flavor of malware before, but we can tell by how it's behaving that it's something that isn't good."

Wellforce also uses network-based AI to scan computer systems for unusual activity. This can help stop attackers before they steal patient data.

Breaches at healthcare organizations cost an average of $408 per compromised record--by far the highest of any sector--according to a July study sponsored by **International Business Machines Corp**. and conducted by **Ponemon Institute LLC.** Financial services, the second highest sector, had an average cost of $206 per compromised record.

About 176.4 million patient records were compromised in 2,149 publicly reported breaches at health care organizations between 2010 and 2017, according to a September analysis published in Journal of the American Medical Association.

The network-based AI tool that Wellforce uses can detect if a particular infusion pump that typically transfers one megabyte of data every hour starts transfering 100 megabytes of data every hour, said Mr. Lehmann.

"We're using AI to detect those needles in a haystack so we can tell our team to go look at those things or take them offline," he said.

Mr. Lehmann said the infusion pump example is not a hypothetical situation for hospital CISOs. "We've seen attacks targeted on infusion pumps… [they] are particularly interesting because there are so many of them and they're all wireless."

Tricking Hackers into Revealing Themselves

Mr. Lehmann also uses a number of tools that focus on deceiving attackers.

"We're experimenting with deception-based AI, which is a special flavor of placing data on a network that looks really interesting and juicy to an attacker, and then monitoring what the attacker does," he said. This technology can help organizations better understand attackers and develop ways to slow them down if they get access to a network, he said.

Another deception tool Wellforce uses is called honeytokens--fake data that appear to be related to the health system--which are placed on the dark web. The honeytokens might be a fake username and password for Wellforce's system, and Mr. Lehmann's team monitors the network for attempted logins using those credentials. The tool is not AI, but intelligence collected from these ploys help the security team surveil their attackers.

"It gives us a sense of how active the search is for the info we have, how bad people want it, where people are coming from when they want to get in," he said.

Erik Devine, the CISO of **Riverside Healthcare**, which services Chicago's southern suburbs, said his organization mostly relies on traditional static defenses, such as firewalls and device identification tools, to protect infusion pumps and other connected equipment. But he is exploring the use of AI to reduce the number of security alerts his staff has to deal with.

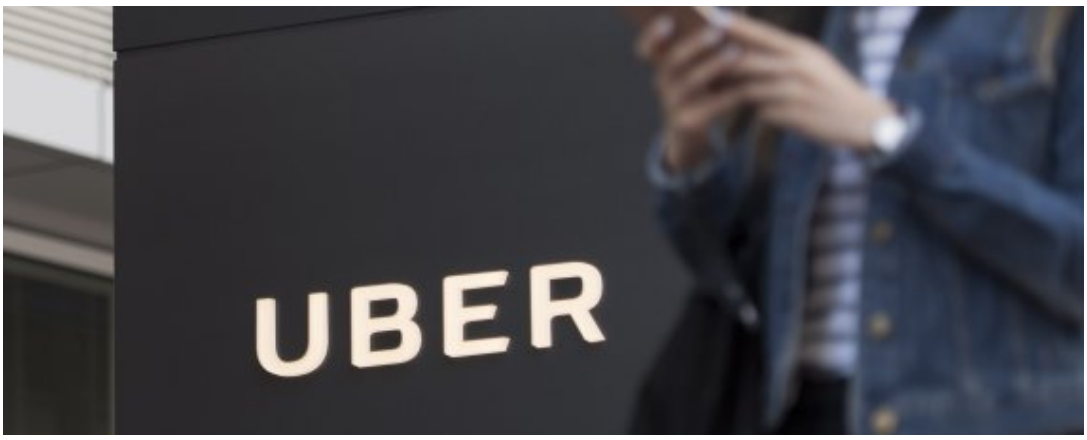
"We're having an issue with how much time do you have to spend making a [security] decision," he said. "You want it to be the right decision, especially in healthcare, and hopefully AI can solve that."

Big Number

176.4 Million

Number of patient records compromised in 2,149 publicly reported breaches at health care organizations between 2010 and 2017, according the Journal of the American Medical Association

More Cyber News



Two hackers allegedly responsible for exposing around 57 million Uber users' data were indicted in a separate data breach case. PHOTO: DAVID PAUL MORRIS/BLOOMBERG NEWS

Alleged Uber hackers indicted in different breach case. Two hackers allegedly behind the data breach of millions of **Uber Technologies Inc.** users have been indicted on separate charges for stealing data from LinkedIn Corp.'s online learning company Lynda, TechCrunch reports. Uber announced in November 2017 that data from around 57 million customers had been exposed more than a year earlier. The company agreed last month to pay a settlement of $148 million. Lynda reported in December 2016 that data from 55,000 of its user accounts was breached.

Financial industry groups create new cyber risk assessment tool. A group of financial services associations and companies have created a new method for banks and other financial services to assess cyber risk, ABA Banking Journal reports. The tool, called the Financial Services Sector

Cybersecurity Profile, uses a questionnaire that members of the coalition expect will reduce the amount of time that financial institutions spend on cyber risk compliance.

Facebook takes down Iranian disinformation. Facebook Inc. announced Friday that it removed 82 pages, groups and accounts that originated in Iran and spread misleading information, the Journal reports. Facebook's head of cybersecurity policy Nathaniel Gleicher wrote in a blog post that the company took down the material quickly because of the upcoming U.S. midterm elections. The accounts targeted Facebook and Instagram users in the U.S. and the U.K. with politically charged posts, including about immigration and Brett Kavanaugh's Supreme Court confirmation hearings. Facebook hasn't found ties between the accounts and the Iranian government, Mr. Gleicher wrote.

About Us

Write to the WSJ Pro Cybersecurity Team: Kim S. Nash, Steve Rosenbush, Adam Janofsky, Jeff Stone, and Catherine Stupp.

And follow us on Twitter: @knash99, @steve_rosenbush, @AdamJanofsky, @jeffstone500 and @catstupp.