ACCUDATA® INSIGHTS
WWW.ACCUDATASYSTEMS.COM

Liars and Cheaters:

How The Ashley Madison Hack Happened

By: Jack Wehman

Ashley Madison sells no products. There are no stores to shop in. There is only a website and a database of paying customers. Their entire company is predicated on retaining and sharing data by fostering private and sensitive communications between paying customers.

And now their business is in shambles, laid low by hackers that released a pirate's ransom of confidential information. 37 million customers had their personally-identifiable information stolen and put on the Internet for anyone to see. And that's not even the full extent of the hack. The company's source code, its proprietary design, was published. The company's email was also compromised.

This isn't some fly-by-night company, either. Avid Life Media, the company that owns Ashley Madison, grossed $115 million in 2014. Pretax profits on that gross income were estimated to be $55 million – an estimate that was made by Avid Life's now-former CEO, Noel Biederman.

Ashley Madison is certainly wishing they spent some of that money on better security – two different law firms have already filed lawsuits for $578 million.

To make matters worse, Ashley Madison touted its security on the front page of its website (and still does!), yet had almost no security at all. Industry experts are speculating that a VPN connection was used to gain root access to Ashley Madison servers – an attack that would have taken no advanced skills to pull off.

"If the breach was truly through a lax VPN password, then it was really an elementary-level attack," said Accudata Systems Principal Security Consultant Kevin Kaufman. "It appears the hackers had unbridled access. Their security was not adequate."

The hacking group known as the Impact Team has claimed responsibility for the attack. Once they were in, they had confidential company and client information at their disposal. No one caught wind of an attacker in the system. It appears no one was monitoring security – which, in today's tumultuous security climate, is like leaving a bank vault open and unwatched.

This kind of attack doesn't fly under the radar. Every time a database is accessed, every time a VPN client starts to transmit data to an external source, a log event is generated. Best practices for a defense-in-depth strategy include monitoring logs and alerts for suspicious behavior. In addition, it is critical to have an incident response process in place to detect and contain a successful intrusion.

Ashley Madison did not have the proper systems in place. Their company's lifeblood was unguarded, unsecured, and unwatched.

"Companies that do not have a way to detect and prevent their data from being scraped have a serious problem," Kaufman said. "It seems like

either no one was watching or no one cared."

Another element of network security is setting strict password and account management policies. It's believed that attackers gained full root access to all of Ashley Madison's servers with the same weak password. Stricter account management and password policies would have reduced this risk.

Implementing privileged identity management to mitigate lateral movement, such as CyberArk's privileged account security solutions, as well as two-factor authentication, would have essentially removed this attack vector in the first place.

"This attack really wasn't that difficult to perform," Accudata Systems Senior Technology Manager Josh Berry said. "Network segmentation is the ideal way to separate your lower-risk assets from your critical assets. In addition, two-factor authentication for remote access has really become an industry standard."

One of the major problems with the Ashley Madison attack was the lack of network segmentation. Once the hackers had access, they could pivot onto other systems in the network with ease – there was little or no segmentation in place to stop them from accessing other systems or servers.

"Implementing network access controls is key to network security," Berry said. "Implementing processes and technology to control and limit admin access in an environment is extremely important."

These types of security holes are typical. They aren't hard to find. A network assessment or even a general IT controls assessment can pinpoint these flaws.

"A network or security assessment is designed to show these kinds of vulnerabilities," Berry said. "We make sure to point out common areas of attack. That's the whole point. We try to find vulnerabilities before the hackers do."

Companies must understand that network security is no longer a luxury – it is a necessity. A company needs network security like a person needs food or water. Cyber-threats like these are only going to increase. You must have the correct people, processes, and technology in place to mitigate cyberattacks when they happen. Anything less means you're eventually going to end up on the front page of a newspaper.

"There are two types of companies," Kaufman said. "Companies that have been hacked and have found out, and companies that have been hacked and haven't found out."

Accudata Systems knows how to protect your network from today's advanced cyber threats. For more information about how Accudata's security experts can help your organization increase security, call 800.246.4908 or visit http://accudatasystems.com/home/services-solutions/security-mobility/.