NEWMEYER & DILLION LLP

C-SUITE BEWARE: CYBERATTACKS ARE TARGETING EXECUTIVES AND FINANCIAL DEPARTMENTS JUST LIKE YOU

By: Casey Quinn and Jeff Dennis

June 7, 2019

Casey Quinn
Contact
702.777.7506
casey.quinn@ndlf.com
Practice Areas
Privacy & Data Security
Appellate Law
Business Litigation
Construction Litigation
Insurance Law

Jeff Dennis
Contact
949.854.7000
jeff.dennis@ndlf.com
Practice Areas
Privacy & Data Security
Business Litigation
Construction Litigation
Insurance Law
Real Estate Litigation

Verizon recently released its 2019 Data Breach Investigations Report (the "Report") and it reveals some startling trends about the targets of cyber breaches. Based on an analysis of 41,686 security incidents, including 2,013 confirmed data breaches, the Report highlighted the increasing number of financially-motivated social engineering attacks. Instead of focusing on installing malware, these attacks focus on credential theft and personal information with the goal of getting unwitting individuals to transfer funds to the attackers. 71% of the breaches analyzed were financially motivated. Not surprisingly, a disproportionate amount of these attacks affect professional, healthcare, and financial industries. The Report is a good reminder that hackers are continuing to get at your company's wallet in new and interesting ways, and, increasingly, are finding that the C-Suite is an easy way in.

The Hacker Mindset

Attackers prefer the use of social engineering tactics in phishing emails to trick users into freely exposing their web-based email credentials. Once the email credentials are in hand, attackers use that access to look for additional targets and methods of compromising the system to their advantage. They look for ways to obtain administrator privileges and move slowly and quietly to map the network, noting weaknesses, and looking for high value targets with which they can abscond.

Their New Targets

Executives, C-Level staff, and financial staff are likely targets. The Report states,

"Overall, these top officers – who typically have access to a company's most sensitive information – were found to be 12 times more likely to be the target of social engineering campaigns like targeted phishing emails and 9 times more likely to be the target of social engineering breaches than in previous years…"

The Report shows that in the professional services industries, financial staff were the most likely to be compromised in 60% of incidents involving fraudulent transactions. But, executives were compromised in 20% of the incidents and are "6 times more likely to be the asset compromised in Professional Service breaches than in the median industry."

Finally, the number of system administrators involved in breaches is increasing—but not by way of the "inside jobs" you might envision. Their involvement is often due to errors made misconfiguring servers in a way that allows unwanted access, or by publishing data to a server that should not have been accessible to all site viewers.

Don't Be a Victim – Protect Your Assets

The good news is that half of all US-based business email compromises had 99% of the money recovered or frozen; and only 9% had nothing recovered. But why risk letting your company end up in that 9%? A few simple steps can significantly reduce your chances of being the victim of a breach:

- Train all employees, from executives to laborers, about proper security practices;
- Where possible, require password managers and two-factor authentication to limit the damage that can be done by stolen credentials;
- Evaluate where you are most likely to be compromised and set up redundant controls, especially with regard to financial matters, so that a single mistake does not result in a breach; and
- Ensure that you have a system in place for administrators to regularly check their work so that any vulnerabilities are quickly resolved.

By taking these steps, your company will be better off when it is targeted. If you want more suggestions specific to your company and line of business, contact us for a consultation.

Casey Quinn is an associate in Newmeyer & Dillion's Las Vegas office, and a member of the firm's privacy & data security practice. Casey brings his substantial experience in complex business litigation to the table, helping businesses proactively navigate the legal landscape of cybersecurity. He can be reached at casey.quinn@ndlf.com.

Jeff Dennis is the head of the firm's Privacy & Data Security practice. Jeff works with the firm's clients on cyber-related issues, including contractual and insurance opportunities to lessen their risk. For more information on how Jeff can help, contact him at jeff.dennis@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For almost 35 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business law, privacy & data security, employment, real estate, construction, insurance law and trial work, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by *The Best Lawyers in America©*, and *Super Lawyers* as top tier and some of the best lawyers in California, and have been given *Martindale-Hubbell Peer Review's AV Preeminent®* highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.