He's paid to break into businesses, and you need to hear what he's learned

SUBSCRIBER CONTENT:
Jul 24, 2017, 7:29am CDT

Jeremiah Talamantes played a video, during a local cybersecurity industry meeting in San Antonio, that he captured while wearing a hidden body camera inside an undisclosed industrial area — what appeared to be an electrical yard.

KRISTEN MOSBRUCKER | SABJ

Jeremiah Talamantes, president of RedTeam Security Corp., offered insight recently to cybersecurity industry professional in San Antonio.

Talamantes — president of RedTeam Security Corp., a cybersecurity company that sells virtual and physical penetration testing — narrated as the video showed him striding across the gravel yard wearing a cloned ID badge, hardhat and work gear when an alarm sounded.

“I was three gates and two [security] guards deep,” he said. “I was thinking security would be coming to arrest me. But they didn’t know the alarm went off, and I got back out just fine.”

Some days, Minneapolis-based RedTeam Security, which was founded in 2010, is hired by corporations to physically try to sneak into executive suites by using social engineering tactics as a way to test and improve security features in the office. Other days, he’s out in industrial sites trying to get inside the main control room and take a few photos for the client, just to prove it can be done. In either scenario, he always carries an authorization letter in case he gets arrested to let authorities know that it’s a drill.

RedTeam Security doesn’t have an office in San Antonio, but it has clients in this market — as well as in Dallas and Houston. Most of the company's clients, which it does not disclose for security reasons, are in the critical infrastructure or utilities sectors.

Talamantes was offering advice on social engineering techniques during CyberDef dojo, a cybersecurity training group in San Antonio that’s supported by local companies like Def-Logix Inc. and SecureLogix Inc.

Social engineering refers to tactics used by unauthorized people — either through email, over the phone or sometimes in person — to gain access to corporate information that can be exploited. In the field, Talamantes said it can be easy to walk into secure areas if a door is held open for someone with a badge, or individuals can tailgate an employee through gates.

It’s not just entry-level workers being caught off guard. Top executives are often the least suspicious because they are often exempt from cybersecurity training. Executives are also some of the biggest offenders when it comes to keeping weak passwords or visible keys to a computer network for the sake of convenience. All of Talamantes’ more than 200 passwords are at least 20 characters long and are managed using a computer application so he doesn't have to memorize them.

“The ramifications of [poor security habits] are happening now because [executives] are not aware of what attacks may look like,” Talamantes told the Business Journal.

That’s because the security “landscape is changing” as cybercriminals go beyond trying to infect systems with malware delivered by email.

Sometimes, bad actors try to get in not only through the back door, but also the front. In that way, security is not just about buying the most expensive technology available, but making sure that it's implemented in practice.

On one occasion, RedTeam Security successfully entered a core building inside an industrial complex that was decked out with a cyberlock system that can cost upwards of $1 million.

“No technology was used other than cloning the [security] badge. I got into all the secret areas without hacking like you see in the movies. It happens all the time,” Talamantes said. “When we ended up breaking in there, what we leveraged was a poorly hung door. So when you think about all the firewalls and things that people put into place, really expensive technology, a poorly hung door is kind of the same thing. It’s a misconfigured server.”

Kristen Mosbrucker
Reporter
San Antonio Business Journal