Feeling safe? Try attending Internet security conference

April 22 2015, byBrandon Bailey

IP addresses are flashed on a screen at the Webroot booth during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. Threat analysts, security vendors and corporate IT administrators have gathered here to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. (AP Photo/Marcio Jose Sanchez)

A conference of Internet security experts is not for the faint of heart.

Hallway chatter and keynote speeches are peppered with scary stories of increasingly sophisticated hackers siphoning off valuable personal and corporate data.

In the words of one expert, the bad guys are outmaneuvering those charged with keeping the wired world safe. This despite repeated vows from CEOs and government officials to tighten security after high-profile breaches at Sony Pictures, health insurer Anthem and retailers Target and Home Depot.

The recent wave of corporate data breaches and cyber-attacks provided plenty of fodder for a weeklong cyber-security conference in San Francisco. Some 28,000 threat analysts, security vendors and corporate IT administrators gathered to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers.

Growing concern over cyber-threats has been good for business, driving up revenue and stock prices for many security firms. But researchers say the dangers are real: Last year saw a record number of commercial data breaches and "denial-of-service" attacks, aimed at shutting down websites by flooding them with bogus traffic.

Here are some highlights from this year's RSA conference, named for its chief sponsor, the RSA security division of tech company EMC Inc.

___

PHISHING WORKS

Attendees crowd around the convention floor during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. Threat analysts, security vendors and corporate IT administrators have gathered here to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. (AP Photo/Marcio Jose Sanchez)

Many data breaches are the result of human error, especially people falling for bogus phishing emails, text messages or websites that appear to come from acquaintances or trusted companies.

Phishing attacks are a favored tactic of hackers working for foreign governments and criminal groups because they trick their targets into handing over passwords or clicking on links that install malicious programs. Verizon researchers estimate one in five phishing emails were read by their targets and one in 10 persuaded someone to open an attached file. Security firm Proofpoint says middle managers are increasingly being targeted with emails containing seemingly "official"

attachments such as fax or voicemail alerts.

"It only takes one person to click" on a link or attachment and put their employer's entire network at risk, said Verizon senior analyst Marc Spitler. As for hackers, "they don't need a high rate of clicking because they can just churn out the emails."

___

CONNECTED DEVICES, EASY TARGETS

As more home appliances are connected to the Internet, experts warn they are vulnerable to hackers intending mischief or worse. While actual hacking incidents have been rare, researchers warn that manufacturers aren't considering security in connected devices.

In separate reports, experts at security firms Veracode and Laconicly said they found vulnerabilities in home systems that control lights, thermostats and garage door openers from a smartphone or other device. While some systems use encryption and other safeguards, the tests found others were vulnerable to hackers eavesdropping on data signals and learning residents' habits, such as what time they leave the house and when they come home.

Patrick Potter, right, chats with Ronald Kent in the RSA genius bar during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. Threat analysts, security vendors and corporate IT administrators have gathered here to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. (AP Photo/Marcio Jose Sanchez)

HACKERS GETTING MORE SOPHISTICATED

Hackers are sharing information about software vulnerabilities in a variety of industries, faster than many companies install "patches" to repair them, several researchers said. Cyber-attackers are also increasingly using programs that can scout a computer network and change behavior depending on what defenses they encounter.

A presentation on web app security is made during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. Threat analysts, security vendors and corporate IT administrators have gathered here to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. (AP Photo/Marcio Jose Sanchez)

Even novice hackers can get their hands on tools to carry out sophisticated attacks. "Writing malware is not the hard part anymore. You can buy it" from other hackers online, said Ryan Olson, intelligence director at Palo Alto Networks.

One common refrain at the conference is that companies must get better at detecting and containing computer breaches once they occur, since old methods of prevention aren't working. The breaches of 2014 showed "that we're losing this contest," RSA president Amit Yoran said in a keynote speech. "The adversaries are outmaneuvering this industry."

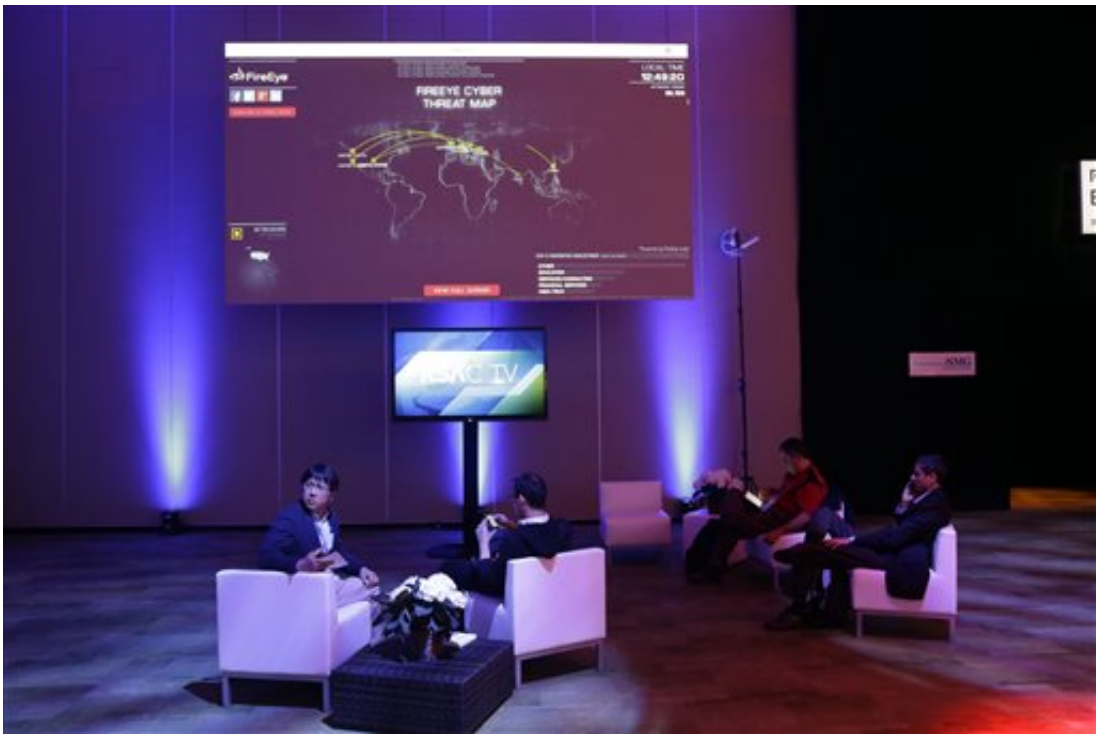
The conference also drew federal officials who urged more sharing of information about hacking attacks. U.S. Homeland Security Secretary Jeh Johnson said his department will open a Silicon Valley office to build partnerships and recruit government workers with cyber-skills.

Elies Campo tries the Oculus Rift Experience, giving the user a 360 degree, 3-D view to travel through a network and clear potential threats, during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. Threat analysts, security vendors and corporate IT administrators have gathered here to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. (AP Photo/Marcio Jose Sanchez)

A man dressed as the movie character Ron Burgundy greets attendees at the Intersect booth during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. Threat analysts, security vendors and corporate IT administrators have gathered here to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. (AP Photo/Marcio Jose Sanchez)

A presentation is made in the Symantec booth during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. Threat analysts, security vendors and corporate IT administrators have gathered here to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. (AP Photo/Marcio Jose Sanchez)

Alexis Papesh takes a break to meditate during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. Threat analysts, security vendors and corporate IT administrators have gathered here to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. (AP Photo/Marcio Jose Sanchez)



A cyber security threat map is displayed inside a lounge during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. Threat analysts, security vendors and corporate IT administrators have gathered here to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. (AP Photo/Marcio Jose Sanchez)

Stijn Vanveerdeghem, at left, an engineer with Cisco, shows graphics with live wireless traffic to FedEx employee Barry Poole during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. Threat analysts, security vendors and corporate IT administrators have gathered here to talk about malicious software, spear-phishing and other attacks that can steal money or secrets from companies and consumers. (AP Photo/Marcio Jose Sanchez)