New Google security chief looks for balance with privacy

April 18 2015, by Glenn Chapman

Google's new privacy and security team chief, Gerhard Eschelbeck is confident his team was up to the challenge of fending off cyber attacks, even from sophisticated operations run by the US National Security Agency or the Chinese military

Google has a new sheriff keeping watch over the wilds of the Internet.

Austrian-born Gerhard Eschelbeck has ranged the British city of Oxford; cavorted at notorious Def Con hacker conclaves, wrangled a herd of startups, and camped out in Silicon Valley.

He now holds the reins of security and privacy for all-things Google.

In an exclusive interview with AFP, Eschelbeck spoke of using Google's massive scope to protect users from cyber villains such as spammers and state-sponsored spies.

"The size of our computing infrastructure allows us to process, analyze, and research the changing threat landscape and look ahead to predict what is coming," Eschelbeck said during his first one-on-one press interview in his new post.

"Security is obviously a constant race; the key is how far can you look ahead."

Eschelbeck took charge of Google's 500-strong security and privacy team early this year, returning to Silicon Valley after running engineering for a computer security company in Oxford for two years.

"It was a very natural move for me to join Google," Eschelbeck said. "What really excited me was doing security at large scale."

Google's range of global services and products means there are many fronts for a security expert to defend. Google's size also means there are arsenals of powerful computer servers for defenders to employ and large-scale data from which to discern cyber dangers.

Eschelbeck's career in security stretches back two decades to a startup he built while a university student in Austria that was acquired by security company McAfee.

What started out as a six-month work stint in California where McAfee is based turned into a 15-year stay by Eschelbeck.

He created and advised an array of computer security startups before heading off to Oxford. Eschelbeck, has worked at computer technology titans such as Sophos and Qualys, and holds patents for network security technologies.

Constant attack

He was confident his team was up to the challenge of fending off cyber attacks, even from onslaughts of sophisticated operations run by the likes of the US National Security Agency or the Chinese military.

Eschelbeck vowed that he would "absolutely" find any hacker that came after his network.

"As a security guy, I am never comfortable," he said. "But, I do have a very strong team...I have confidence we have the right reactive and proactive defense mechanisms as well."

State-sponsored cyber attacks making news in the past year come on top of well-known trends of hacking expressly for fun or profit.

The sheer numbers of attack "vectors" has rocketed exponentially over time, with weapons targeting smartphones, applications, datacenters, operating systems and more.

"You can safely assume that every property on the Internet is continuously under attack," Eschelbeck said.

"I feel really strong about our ability to identify them before they become a threat and the ability to block and prevent them from entering

our environment."

Scrambling data

Eschelbeck is a backer of encrypting data, whether it be an email to a friend or photos stored in the cloud.

"I hope for a time when all the traffic on the Internet is encrypted," he said.

"You're not sending a letter to your friend in a transparent envelop, and that is why encryption in transport is so critical."

He believes that within five years, accessing accounts with no more than passwords will be a thing of the past.

Google lets people require code numbers sent to phones be used along with passwords to access accounts in what is referred to as "two-factor" authentication.

The Internet titan also provides "safe browsing" technology that warns people when they are heading to websites rigged to attack visitors.

Google identifies about 50,000 malicious websites monthly, and another 90,000 phishing websites designed to trick people into giving up their passwords or other valuable personal information, Eschelbeck said.

"We have some really great visibility into the Web, as you can imagine," he said.

"The time for us to recognize a bad site is incredibly short."

Doubling-down on privacy

Eschelbeck saw the world of online security as fairly black and white, while the privacy side of his job required subjective interpretations.

Google works closely with data protection authorities in Europe and elsewhere to try and harmonize privacy protections with the standards in various countries.

"I really believe that with security and privacy, there is more overlap than there are differences," he said.

"We have made a tremendous effort to focus and double-down on privacy issues."

As have other large Internet companies, Google has routinely made public requests by government agencies for information about users.

Requests are carefully reviewed, and only about 65 percent of them satisfied, according to Google.

"Privacy, to me, is protecting and securing my activities; that they are personal to myself and not visible to the whole wide world," Eschelbeck said.

Citation: New Google security chief looks for balance with privacy (2015, April 18) retrieved 22 September 2024 from https://phys.org/news/2015-04-google-chief-privacy.html