Beat: Business

APPLE(Gate) & FBI:THE 800 LBS GORILLAS AT RSA

HACKING, ENCRYPTION, SECURITY & THE LAW

San Francisco, 08.03.2016, 02:44 Time

USPA NEWS -

RSA 2016 was kicked off last week in San Francisco by president Amit Yoran. In his opening remarks he told attendees: "Our problem isn't a technology problem. Adversaries aren't beating us with better tech. They're beating us because they're being more creative, more patient, more persistent"

As expected, the ongoing dispute between Apple and the FBI resonated throughout the conference. The FBI wants Apple to turn off a security feature that disables the phone after 10 failed password attempts. When the phone is locked, the data is encrypted. Apple has argued that breaking the encryption would not only be a significant technical challenge but a threat to both its First Amendment and Fifth Amendment rights.

While not mentioning Apple explicitly, Yoran´s support of the company's stance quickly became very evident. "Weakening encryption is solely for the ease and convenience of law enforcement," said Yoran. "If we weaken our encryption, you can be sure the bad guys will use it against us. A succession of keynote speakers made their alliances clear, agreeing with Apple's perspective that developing a backdoor that would let the FBI circumvent encryption and access the phone's contents would be akin to opening Pandora's Box.

One of the most outspoken supporters, Brad Smith, president and chief legal officer for Microsoft emphasized: "When it comes to security, there is no technology that is more important than encryption. The path to hell starts with the back door, and we need to ensure that encryption technology remains strong.“

Smith offered up a previous unshared revelation. Following the Paris attacks last year, Microsoft received 14 requests from law enforcement seeking access to data related to terrorists who were at large at the time in France and Belgium, and Microsoft validated those requests and replied to each one in an average of 30 minutes.
But he said that cases like the Apple vs. FBI flap risk the public's trust in future technologies and the companies that create them.
"You can't advance technology without trust," said Smith. "The world is going to trust technology only if the law can catch up."
The outcome of Apple's battle with the FBI could go a long way toward helping with that process.

Attorney General Loretta Lynch addressed the controversy surrounding Apple´s refusal to break the encryption on an iPhone that belonged to San Bernardino terrorist Syed Rizwan Farook. She expressed surprise that since Apple has cooperated with FBI requests in the past“”and continues to do so on other matters“”that in this specific case Apple´s response has been to say “we´re done.“

While reluctant to criticize Apple or Cook directly, Lynch did ask the audience of security pros here whether they wanted to “let one company, no matter how beautiful their devices are, decide this issue for all us. We don´t do that for any other industry.“ She suggested there might be other ways to get the information the FBI is after, but she said Apple doesn´t want to discuss the issue with law enforcement any further. “I respect their position. Tim Cook and his views will be decided in court,“ said Lynch.

As for the Fifth Amendment protection against self-incrimination Lynch said: “Apple is not a target in this matter. We´re not alleging Apple has done anything wrong, they are a third party in this.“ In earlier prepared remarks, Lynch made a plea for more cooperation and partnership with the public sector to combat growing cyber threats. “We are committed to working closely with the private sector, some of our most fruitful conversations have been with you,“ Lynch said.

According to Scott Borg, Director of the U.S. Cyber Consequences Unit if the government is allowed to force Apple to provide access to iPhones in this case, they will be able to do it again. “If the government is given tools for accessing iPhones with any regularity, we have to assume that these will be stolen by Russian intelligence and eventually by Chinese intelligence and other intelligence agencies. If the Russian and Chinese intelligence agencies have tools of this kind, these tools will eventually find their way into the hands of organized crime.“

Therefore, Mr. Borg concluded, that what the FBI is proposing could eventually result in our smart phones becoming accessible to hostile, authoritarian governments and to criminals. “Meanwhile, terrorists and serious criminals will still be able to hide their activities from the government, because they can easily download open-source encryption tools that even the major intelligence agencies have not been able to crack. From the standpoint of privacy and secure communications, this could be the worst of all worlds.“

Google, Microsoft and Adobe executives took on the issue, and they made one thing abundantly clear: Privacy is an often-foggy topic that presents numerous challenges and requires some uncomfortable tradeoffs. One of the primary obstacles identified is exactly how to define privacy and the role it plays within an organization. The answers are different for every entity, depending on factors such as industry, product type, customer profile, and compliance requirements. "It's about what's appropriate collection, appropriate protection and appropriate use," said Brendon Lynch, chief privacy officer at Microsoft, describing the prism through which the company views privacy. "Sometimes privacy and security work hand-in-hand, sometimes they're treated as separate processes."

Another hot topic, with the emergence of Internet of Things (IoT) and the rapid acceleration of digital and converged systems, security professionals are challenged with identifying risks related to business critical assets without stifling innovation. The assessment of IoT devices along with the need to mitigate risks associated with IoT is prompting organizations to gain visibility into network traffic generated by these connected devices. s this to be a significant driver of growth in the security information and event management segment from $1.7 billion in 2014 to $2.6 billion in 2019, as organizations look to build security and analytics capabilities into the deployments of emerging technologies.

Fitting the occasion, Hewlett Packard Enterprise responded and announced new security offerings designed to help organizations build protection into the fabric of their enterprises and stop attacks through comprehensive detection and response capabilities. Chandra Rangan, Vice President Marketing, HPE Security Products at Hewlett Packard Enterprise focused on the importance of an end-to-end data encryption solution designed to protect sensitive information in mobile environments. This solution expands upon the HPE Secure Data product portfolio, enabling organizations to build data security into their mobile applications and safeguard the data throughout its full lifecycle "" at rest, in motion, and in use.

Highlighting importance of socially-engineered behavior which is to blame for most security breaches security, Sandy Vandebult, CIO of Awareness Training firm KnowBe4, LLC stressed the importance of employee soft skill training. The company has released an analysis of 372 organization that clearly shows the impact and effectiveness of Security Awareness Training on employees. The study was done over a 12 month period and follows behavior patterns of 291,000 end points, showing a reduction in risky behavior by over 12X. Using an initial baseline of 15.9% for the "phish-prone"? (employees prone to click on dangerous phishing links), training methods used by KnowBe4 reduced this to a 1.28% average.

Article online:
https://www.uspa24.com/bericht-7303/applegate-und-fbithe-800-lbs-gorillas-at-rsa.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Ina von Ber

Exemption from liability:
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report. Ina von Ber

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619