EU ministers rattle sabres at encrypted ISIS jihadi comms channels

Aug 23, 2016
News by Adrian Bridgwater

France and Germany discuss 'tapping' encrypted end-to-end networks such as WhatsApp and Skype

Tweet

French interior minister Bernard Cazeneuve is due to meet his German counterpart, Thomas de Maizere this month (August 2016) to discuss new measures that could result in a limitation in the use of encrypted communications across the EU. Cazeneuve has already told the press that he regards this as a, "central issue in the fight against terrorism."

Existing methods including phone tapping are now thought to be somewhat outdated in an age where online communications platforms exist in so many multifarious forms.

The problem, or at least one of the major difficulties here, is that applications built with end-to-end encryption functionality as a default part of their architecture (such as Facebook's WhatsApp and Apple's iMessages) are now extremely difficult (some sources argue almost impossible) for Europe's intelligence services to read.

If implemented in full, it is thought that new European Union online communications tapping powers could also extend to Skype.

The jihadi comms channel?

According to the Financial Times, "As details of the interlocking Isis terror cells responsible for the Paris and Brussels attacks have emerged, it has become evident that such encrypted messages are vital to how jihadis prosecute their violence in Europe."

Jacob Ginsberg, senior director at encryption company Echoworx questioned the privacy element of proposed developments and asked how far new laws may be putting the majority of law abiding citizens at risk. He argues that European lawmakers need to remember that cyber-surveillance is no different than old school wire-tapping.

"However," says Ginsberg. "The government requires court approval for a wiretap and only after they have demonstrated evidence of reasonable suspicion. They should not be allowed to circumvent existing laws based on type of media under surveillance."

Ginsberg argues that these laws were put in place to protect the average person from this kind of intrusion. "The same rules should apply regardless of whether its phone conversations or web and social media use being tapped. There is a balance that needs to be struck but it is absolutely vital that there is appropriate judicial oversight dictating the use of these powers," he said.

Backdoor weaknesses

Security researcher Junade Ali spoke to *SCMagazineUK.com* directly in line with this story to say that it is worth noting that when an encryption system features a backdoor, such as for law enforcement access, it may be made insecure.

"The point of encryption is to make it mathematically impossible for anyone else, but the intended recipients, to read the message. Backdoors make it possible to exploit this, whether the system or keys (that) law enforcement use to access the backdoor are cracked or leaked," he said.

Ali advises that governments may find it challenging to compel international companies, whilst driving encrypted communication businesses out of their own countries.

"This also fails to address open-source encryption systems, given how publicly accessible encryption implementations are these days. Furthermore, terrorism powers have been abused before. Examples of this include Section 44 of the Terrorism Act in the UK and more recently Human Rights Watch has documented some abuses of the French State of Emergency," he said.

A weakness for everyone

Brian Spector, CEO at Internet cyber-security company MIRACL (Multiprecision Integer and Rational Arithmetic C) spoke to *SCMagazineUK.com* to say that these proposals wouldn't just make it easier for governments to spy on their citizens; it would also weaken the very products and standards that we all use to protect ourselves.

"Successive governments believe that they can manipulate security in such a way that only they can take advantage of that subversion. But this is a fallacy. The same technologies, standards and products are used by everyone, so we either allow everyone to spy on everyone, or prevent anyone from spying on anyone. If we insert vulnerabilities, we weaken security for everyone. The same vulnerabilities used by intelligence agencies to spy on global citizens can also be used by criminals to steal your passwords. We either enable spying - by either governments or hackers - or we defend against it," he said.

Spector says that going forward, this kind of mentality will make us all less safe. "Quite apart from damaging the products and technologies in question, it can damage trust in the Internet entirely. In order for the Internet to continue to grow, users need to believe that the systems they use online are not part of a government programme to spy or snoop on its citizens," he added.

Topics:

- Surveillance
- Privacy
- EU
- Encryption
- Regulation

MORE FROM SC MEDIA UK

Are we ignoring the collateral damage of encryption?

Are we ignoring the collateral damage of encryption?

Nine out of 10 UK orgs don't encrypt over 75% of data in the cloud

Nine out of 10 UK orgs don't encrypt over 75% of data in the cloud

Video explainer: What's wrong with encryption back doors?

Video explainer: What's wrong with encryption back doors?

More on this Topic

- One fourth of global organisations faced breaches because of unpatched vulnerabilities
- Cyber-crime thrives on legal inefficiency & business leaders turning a blind eye
- APT10 campaign debuts two new loaders for distributing PlugX and Quasar RATs
- Assange indicted on 17 counts under Espionage Act
- Unsecure Chtrbox AWS database exposes data on 49 million Instagram influencers, accounts