Paris Call: Important Commitment Against The Arms Race With Cyber Weapons

The following text by Ninja Marnau was published on 14.12.2018 in the Tagesspiegel - Background Digitalisierung (in a shortened version) under the title "Disclosing security vulnerabilities instead of selling them ". It is a reply to an op-ed on the Paris Call.

On 9.12.2018 the Tagesspiegel published the opinion piece "About the myth of the evil hacker" (German). In this opinion piece Dr. Sandro Gaycken criticises the "Paris Call for Trust and Security in Cyberspace", an international agreement in which the signatory states commit themselves, among other things, to comply with voluntary standards for the responsible handling of IT security vulnerabilities during peacetime. The agreement, led by French President Emmanuel Macron, also calls for government measures to increase overall IT security and to disclose discovered IT security vulnerabilities responsibly instead of using them as investigation tools and cyber weapons.

Gaycken claims that disclosing security vulnerabilities to software and hardware manufacturers does not improve overall security. There would always bugs and vulnerabilities and since the "bad hackers" use them anyway, it must also be made possible for the "good hackers". Gaycken's depiction of IT security is deeply fatalistic. And false.

First of all, IT security vulnerabilities do not exist in a "darkness of ignorance". They can be systematized and evaluated. We also know how and why they occur, both technically and economically: Poor or not security-oriented design, cost and time pressure, lack of expertise and diligence during development and implementation, growing complexity, networking and dependencies, etc. Every day, several hundred research teams worldwide work systematically to find and close unknown security vulnerabilities. However, if they succeed, they are in a conflict. If they notify the manufacturer of the discovered vulnerability, they will at best receive a small financial reward or can write a publication for their scientific CV. In the worst case, they receive a reply from the company's lawyer. At IT security conferences, however, the researchers are courted by companies that buy critical and undisclosed vulnerabilities (so-called "0days") for large sums of money in order to sell them on to governments. On this grey market of security vulnerabilities, millions may be demanded and paid.

Some of these companies also sell to autocratic and human rights violating states, either to monitor their own population or to spy on and attack enemy states. Gaycken writes that limiting the offensive IT attack possibilities of European states by disclosing vulnerabilities would lead to massively asymmetrical disadvantages compared to more “cybertechnically active” states or authoritarian regimes such as Russia, China and the USA. This is as platitudinous as it is true. However, this realpolitik arms race should not be the only contributing factor in dealing with security vulnerabilities for EU member states. If countries like Germany participate in buying security vulnerabilities, they will further fuel this grey market and more researchers will decide to sell their results rather than publish them.

Usually, The manufacturers and users remain uninformed about the security vulnerabilities that are traded in this way, in order to allow secret services and the military to use the vulnerabilities for as long as possible. On average, these secret vulnerabilities remain exposed for seven years. Meanwhile, they can also be discovered or bought by criminals and anti-democratic states. The probability of discovering the same vulnerability in parallel is much higher than one would assume, between 6 and 23%. So while states and criminals operate with IT security vulnerabilities, the only ones who are unaware of the vulnerability and therefore cannot protect themselves are manufacturers and users.

It is another misconception to believe that the security vulnerabilities would be safe with government agencies. These are building blocks for cyber-weapons and therefore attractive targets for hackers and insider threats. In recent years, the hacker group The Shadow Brokers has published several classified NSA attack tools, including 0day attacks. One of these known security vulnerabilities was later exploited for the global WannaCry attack.

The responsible disclosure of security vulnerabilities, on the other hand, can lead to an actual increase in IT security in the long term. For example, the "Heartbleed" vulnerability, a catastrophic flaw in website encryption, was patched within a week of its disclosure in 2014. Within a month, almost half of the half million affected web servers were secured. Depending on the media attention given to a security vulnerability, a rapid and comprehensive improvement in system security can actually be achieved.

However, the Heartbleed example also shows where there is still room for improvement. Since the first month after the disclosure, activity in terms of securing website encryption dropped significantly: in 2017, around 200,000 web servers were still vulnerable, including 14,000 in Germany. Hence, how operators can be better informed and assisted to react quickly to known security vulnerabilities is part of our current research at CISPA. Every user and operator must become active, use up-to-date software and install security updates as soon as possible. For these measures to be effective, however, the government must also handle security vulnerabilities responsibly.

The Paris Call calls for nothing more than this responsible conduct. It does not demand unconditional or immediate disclosure, but sensible vulnerability management by the government. In order for intelligence services and prosecutors to receive information in a justified individual case, proverbial "cyber sledgehammers" are required in very few cases to crack a nut. In the remaining cases, for which the German Central Office for Information Technology in the Security Sector (Zitis) is looking for 0days to equip German prosecutors and intelligence services with offensive IT tools, we need rules to decide whether a vulnerability is so critical that the manufacturer must be notified and when and how this should be done. The Paris Call is therefore an important European declaration against the state arms race with cyber weapons, which endangers the security of us all.