Ignorantia IT nocet,

or a few words about the consequences of the unwitting use of new technologies

Jakub Kralka,
Product Manager Axence

In today's article we bust some myths, present facts and discover hackers' tricks; all with purpose of educating you on how to move about the Internet in a secure way. In the interest of limiting the number of failures and attacks, often resulting from the unwitting behavior of the employees, please read and, if necessary, publish this article in the Knowledge Base of the Axence nVision® HelpDesk module.

The revolution, which started by the launching of websites and making them available to the public, enabled millions of people to access a powerful work and development tool. However, each tool, when used incorrectly, can cause more damage than good. Taking into consideration that the weakest link of each IT infrastructure was, is, and for a long time will be its user, the potential risk rises. Let us use a few examples to illustrate the vast number of traps awaiting you in the network.

1. The risk of being attacked is negligible. The Internet is huge. Why would someone target my computer or phone?

Just as fishermen, hackers often release their malware into the wide world and wait until someone gets caught in the net: will hit a data stealing website, will connect to an unsecured hotspot capturing data transmission and recording logins and passwords, or will install a disk encrypting malware. These are largely automated attacks, performed by well-organized criminal groups, equipped with hardware and knowledge.

2. Free does not mean good

Free applications from unknown vendors, especially those developed for open source systems[1], expose us to potential data loss and the last remnants of privacy. An example is the series of approvals for access to information on your smartphone or tablet you need to give when you want to install a new app. For instance, we rarely think about why an application grouping news from the services we are interested in, requires access to our:

- SMS messages,
- contact list,
- microphone,
- photo gallery,
- location,
- disk resources,
- notes,
- etc.

3. I am safe, because I have nothing to hide, no one cares about me because I am an average Joe

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about freedom of speech because you have nothing to say"[2]. The notorious affair of Edward Snowden, accused of treason, proves how often we are invigilated by intelligence services operating officially and at the request of state authorities. However, our workstation or mobile device may be used as a gate, leading the hacker inside the infrastructure they would like to, but cannot penetrate due to security measures. Lack of BYOD policy may result in letting a theoretically trusted person with a malware-infected device into our network.

4. Public Wi-Fi networks must be protected

We do not and we should not have any grounds to suspect that the institutions providing a hotspot on their premises have any bad intentions. However, any person with a little knowledge of the scope of broadly understood IT, Internet access and $100 to spend, can legally buy a tool imitating an open hotspot, which allows the full transmission of a user to be captured[3].

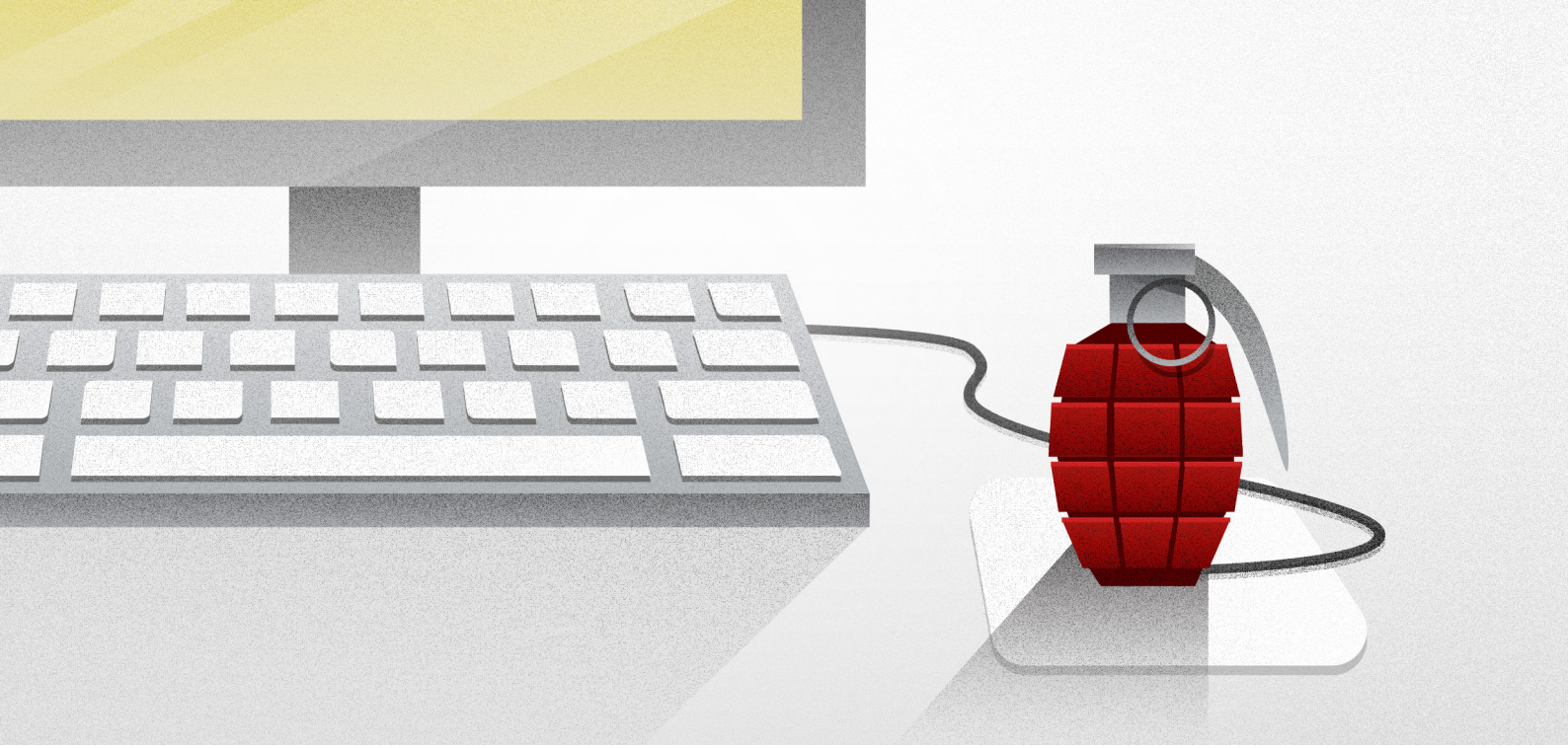
5. Another update?!

We are often flooded with notifications about available updates for the various systems we often use. Regardless of whether these are operating systems, browsers, messengers or other software, their updates have two primary purposes: to optimize operation and add new features, and to raise the security level related to their use. Gaps in applications and utility systems, patched by the developers with updates, are used by "zero day" attacks, resulting in data loss or the opening of the corporate network to third parties.

[1] https://www.welivesecurity.com/2017/02/20/trends-android-ransomware/

[2] https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/

[3] https://hakshop.com/collections/wifi-pineapple-kits/products/wifi-pineapple?variant=81044992



6. Hacking attacks are only a scare, specially inflated to keep me under control

The fact the users have learnt the security policy does not necessarily mean they have understood what they read and undertook to follow it. Moreover, despite reports on the more and more audacious actions of the cybercriminal groups, employee behavior remains unchanged, and they still do not realize that they make themselves and the infrastructure vulnerable to losses. According to PWC, 96% of companies experienced more than 50 security violation incidents in the last year, and a phishing attack is the most common security violation incident in companies. 79% of most of these incidents are caused by current employees[4].

7. I'm making backups – I'm protected

How many administrators or users check whether the performed backup can be restored without data loss? Are the backup-related devices properly secured? You need to remember that security is a process, not a final product[5] and you can NEVER be sure your infrastructure is 100% secure.

This is what each day looks like: you get up, have your morning coffee, you browse popular news sites, and social media. You often do it on your company hardware. A friend just found an interesting new portal, and your girlfriend liked a new app. Sometimes you click the suggested source without much consideration. This is only one of many scenarios where your computer or smartphone can get infected. Let us be wary, and the above examples of the incorrect way of thinking about network threats should make us sensitive to – often tragic - consequences.

[4] https://www.pwc.pl/pl/pdf/ochrona-biznesu-w-cyfrowej-transformacji-pwc.pdf

[5] https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html