Security Advisory 2021-017

Straightforward Rules for Perfect Cyber Security

April 1, 2021 — v1.0

TLP:WHITE

History:

- *01/04/2021 — v1.0 – Initial publication*

Summary

Throughout several years, CERT-EU has been investigating thousands of cybersecurity incidents. These ranged from simple cases of phishing, through compromise of internet-facing IT assets, and up to highly sophisticated Advanced Persistent Threats (APTs). Based on this large volume of examples, CERT-EU has been able to perform a very **careful and in-depth analysis** of the underlying reasons that lead to these cyber-incidents.

Thanks to this groundbreaking, Human Intelligence powered research, CERT-EU managed to identify **basic and straightforward rules** that – once implemented – will allow anyone to achieve **perfect cybersecurity** in any organisation:

- **Rule no. 1: Use only secure software.**
- **Rule no. 2: Install efficient filtering solutions.**
- **Rule no. 3: Allow users to perform safe actions only.**

These rules are extremely simple to implement and **do not require significant budget or resources**. It is also trivial to **ensure compliance** requirements as well as **save money** on any other (completely unnecessary) security provisions.

Technical Details

This section focuses on the practical, ready to use implementation of the general rules presented above.

Use Only Secure Software

Generally speaking, the term *secure software* is used to denote designing, building, testing and deploying software so as to reduce vulnerabilities and to ensure the software's proper function when under malicious attacks [1]. The consequences of using software that is not secure could be dire [2], hence this should be absolutely avoided.

Here are easy to follow, practical steps that would ensure that only secure software is used in an organisation:

- Carefully choose commercial **software vendors that only provide secure, vulnerability-free software** – for obvious reasons, it is inefficient (and insecure!) to buy software that is not secure or contains vulnerabilities.
- When using community-supported or open-source software – **ensure that the software is secure** before making a decision to deploy it. With open-source software, this is easy and can be done with a simple script, such as:

```
#!/usr/bin/env python

with open('source_code') as source:
 assert source is secure, 'Error: Source code not secure!'
```

- **Use only secure configuration**. Some software requires configuration after having been installed – examples include web servers, file sharing servers, etc. To ensure safe and flawless operation, only a secure configuration must be used.
- **Do not update** the software once it is installed – **secure software does not need security updates**, which dramatically reduces maintenance and the total cost of ownership.

Install Efficient Filtering Solutions

Even with the successful implementation of Rule no. 1, it is still possible that an organisation may be threatened by malicious external activities against their perimeter [3], such as spear-phishing, spam, DDoS attacks, and many others [4]. This is why our second identified basic rule is so important.

In order to entirely mitigate any such risks, the following steps need to be followed:

- **Install basic, but efficient filtering mechanism** on the perimeter of your network. This mechanism needs to follow very basic filtering rules, such as this example SNORT rule:

```
block any any any -> $my_network (is malicious?)
```

Please note that filtering defined this way is **not blocking any outgoing packets**. This is intentional, as the **internal infrastructure is completely safe thanks to implementing Rule no. 1**, and no user action can endanger the security of the organisation thanks to the implementation of Rule no. 3 below.

Allow Users to Perform Safe Actions Only

The perfect security posture of an organisation would not be complete without proper user awareness and collaboration. Even with entirely secured software (Rule no. 1) and protected from any external threats (Rule no. 2), users' action could still inadvertently lead to disastrous outcomes [5].

Fortunately, there is an easy solution for this problem – **users should only be allowed to perform safe actions**, i.e. only actions that do not lead to issues, problems, security risks, or data compromise or exfiltration. Any **other actions must be strictly prohibited**.

Recommendations

The recommendation is straightforward. **Deploy in your organisation rules 1 through 3 as soon as possible**, and enjoy a perfect cyber-secure environment!

Happy April Fools' Day and stay safe (and sane)!

References

[1] https://study.com/academy/lesson/secure-software-definition-characteristics.html

[2] https://insights.sei.cmu.edu/cert/2017/06/the-consequences-of-insecure-software-updates.html

[3] https://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf

[4] https://sendgrid.com/resource/phishing-doxxing-botnets-and-other-email-scams-what-you-need-to-know/

[5] https://www.helpnetsecurity.com/2019/10/08/internal-user-mistakes/