SecurityGen

Telecom Security. Transcending Generations.

Early Threat Identification Works and Helps Telecom Business Develop Further

www.secgen.com

This paper covers the following points

1 Early threat identification

Objectives and examples of early threat detection going a long way in proactive security coverage

2 Use cases & facts

How exactly early threat identification can help prevent exploits, data leaks and enhance the security posture

3 Conclusion

Why implement early threat identification; if you have not done it yet, or how to improve if you have a process in place.

1 Early threat identification

1.1 Objective of early threat identification

It doesn't take a genius to know that the earlier a problem is detected, the greater its chances of being fixed efficiently, and in a cost-effective manner. Health check-ups offer the best analogy in this regard, and the same holds true for technologies, information systems, and businesses. In this case, the telecom businesses. Early threat identification is created to solve the following tasks:

It really works this way.

1.2 Let's consider the following basic tasks that early threat identification can help resolve:

Estimate threats and find proper mitigation

It would be foolish to assume that the entirety of time and budget can be spent on resolving cybersecurity issues. That's partly because the volumes are massive and increasing, and nothing is forever water-tight. Supporting a company does not mean fixing everything. It just means tackling highly critical threats in a prioritized, and timely, manner. That is what makes identification and verification of threats efficient: it automatically provides information on how to manage cybersecurity priorities – the threat that is real must be addressed.

Address the issue before it strikes

Limiting the number of threats to be addressed, will help you plan the "what, how, and when" of resolutions. This ensures a proper response – whether it is hardening, additional security controls, deployment of protective solutions of updated playbooks and procedures. And of course, it is a well-thought-out remedy, should the incident still occur.

Apply the most efficient solution

This is common sense. The 1/10/100 rule states that prevention is less expensive than correction, and correction is less expensive than failure. It always makes more sense to invest $1 to prevent an incident than spend $10 on a correction. Furthermore, it makes more sense to spend $10 on correction than $100 in the event of failure.

2

Use cases & facts

2.1 Early threat identification increases security posture and resilience to cyber-attacks and fraud

Every mobile network is a comprehensive ecosystem - network elements of various vendors, interconnecting links, and a host of configurations. Constantly controlling the assets is an imperative in such complex ecosystems.

Given the scale of such a landscape, it is critical to focus in the right direction in terms of security implementation. That's why it's important to tackle confirmed threats and verified vulnerabilities first. In this regard, assessing the network properly is pivotal. Armed with the list of confirmed threats and proven vulnerabilities, information security personnel can analyze and estimate potential risks and money losses, prioritizing them accordingly. Justification with proof makes it easier to get the budgets for the required software/equipment and plan configuration changes with other departments. In all, this improves the security level of the network.

The network security assessment process should be undertaken regularly since networks are constantly evolving. The earlier a new threat or vulnerability is identified, the better the network's chances of gaining resilience before an attack occurs.

2.2 The simplicity and cost-effectiveness of finding and fixing a problem beat hands-down the consequences of a vulnerability being exploited

Let's take the example of A2P fraud. Peer-to-peer SMS may be a thing of the past, but businesses pay for Application to Peer (A2P) SMSes, as much to attract new clients as to serve existing ones. A2P SMSes offer enterprises the benefit of tapping into a well-working channel for client communication. For mobile operators, it presents the opportunity to utilize an old, but well-working, service and sell it at rates higher than P2P SMSes. If malefactors find a vulnerability in an MNO's network, which allows them to terminate SMS by bypassing the operator's billing

systems, they get an opportunity to keep all the profits from the A2P SMS delivery. The victim is the MNO, as they provide all the services but get none of the profit. Losses to the operator might run into several hundred thousand USD per month.

Data from proven resources:

$12 billion+ The annual estimated cost of telecommunications subscription fraud in 2020 (1).

$7.9 billion was lost due to grey routes from a total of US$19.4 billion generated on A2P in 2021 (2).

1-2% of telecom revenue loss is due to costs associated with network fraud(3).

Some say it has been difficult to prevent because it requires fraud intelligence to be exchanged at great speeds. But in many cases, it may be prevented if the root cause is addressed. That's why it is important to give proper cyber-security the importance it deserves, that ensures:

- Timely identification and proper analysis of vulnerabilities
- Mitigation of threat of fraudulent activity and illegal monetization
- Additional revenue generation, and reduction in monetary losses

2.3 Increased cost of breached accounts and violated private data

Two-factor authentication is a common technology that ensures additional protection during actions such as service login, personal confirmation for offline actions, or banking transaction approval.

What service providers often overlook is that the second factor of authentication is an additional security measure, not a standalone one. If that happens, 2FA interception could well lead to detrimental consequences.

Businesses often use SMS as a media for 2FA, as this technology is relatively cheap and mobile devices are widespread.

If 5 years ago an SMS interception to attack a bank looked like a fantasy, today it has already started becoming a mainstream fraud.

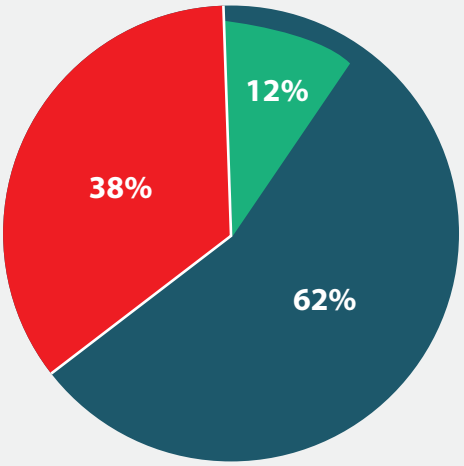
Unlike the SMS A2P traffic fraud, the profit of the malefactors from this kind of action might grow up dramatically because the fraudsters get access to the banks, e-wallets, crypto brokers, personal accounts, and government systems.

This brings to the fore another challenge pertaining to personal data: GDPR. If a mobile operator in the EU leaks the personal data of users, the operator would run the risk of being **fined up to EUR 20 million or 4% of the annual operator's revenue.** GDPR has stringent compliance requirements and there are a number of European operators who have already faced heavy fines due to the violations.

According to information available in the public domain about fines imposed by the DPA, (4), there is already a long list, with violators being fined variously from **EUR 10,000** – for a data leak that allowed unauthorized third parties to get access to it – and **up to EUR 6 million** for massive data leakage. **The reason? Failure to implement adequate technical security and organizational measures to ensure proper execution.**

2.4 Inefficient security measures leave networks exposed to cyberattacks

Results of friendly offensive testing for different mobile operators across the globe show the number of implemented security solutions (for instance signalling firewall) increasing every year, though there hasn't been significant improvement in the security level.



Which

Indicates

38%

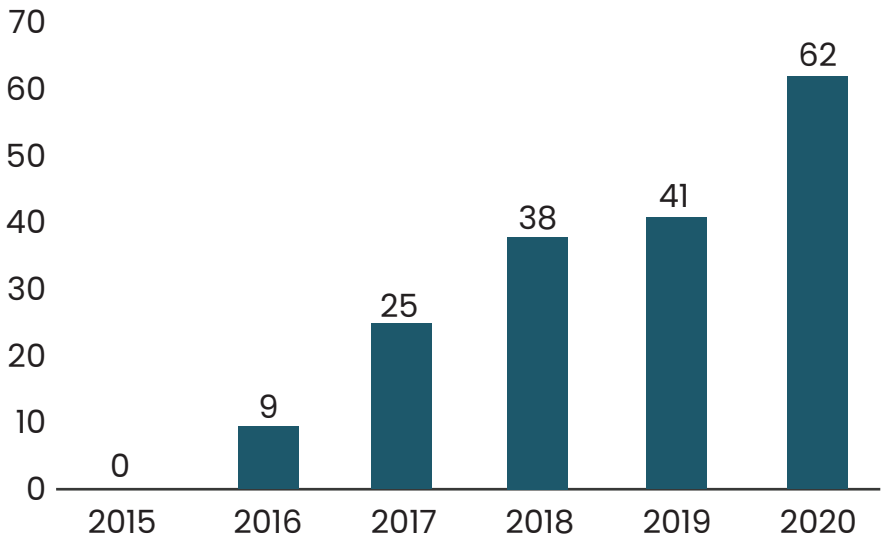
Totally Vulnerable

50%

Partially Vulnerable

- Analyzed networks which had implemented security solutions on their premises
- Totally vulnerable
- Really protected

* Data source : 2020



(cart) – % Security solutions in place in MNO Core networks

Introducing a security solution into the network isn't enough by itself. Ensuring it is properly tested and integrated is just as important. For instance, while the signalling firewall might be working properly, an incorrect routing on a border STP might undermine overall security.

That's why it is important to assess the security level of the network after the means of protection are made operational.

Another factor that influences security is the eternal evolution of mobile networks. These are constantly, fine-tuned, and upgraded, with new services and equipment being introduced regularly. Yet, the improvements aimed at making the network more robust, efficient, and fast also may affect security. This is the reason a good security officer should check the health of security periodically throughout the whole network lifecycle. If a system upgrade affects security, the officer responsible will be able to identify this issue on time and take steps for protection before intruders exploit the vulnerability.

3

Conclusion

This is where we should start. Early threat identification, just like health check-ups, is the main exercise to identify the potential issue as early as possible, it provides a greater chance to address the issue efficiently, and in a cost-effective manner.

There are many cases:

- If you are unsure that the current security posture of telecom network and core infrastructure elements is adequate. An early threat identification process will show the actual state and guide toward a better security posture.

- If you feel comfortable with current security state, but you realize that upcoming changes in business digitalization and 5G deployment will increase security requirements - Early threat identification will help to achieve higher results.
- If you've already organized early threat identification for IT assets and feel confident about results – scaling the process to telecom network and core infrastructure elements will help achieve similar and better results for assets that were not covered before, and guarantee status quo of security for the entire company.

Early threat identification and verification should be the mandatory activity in a comprehensive cybersecurity framework for telecoms. The current speed of implementation of new technologies and services also requires a high frequency of such analysis to spot critical deficiencies and vulnerabilities.

Therefore, the approach of automated Breach and Attack simulation for telecoms should be the most suitable option.

References

1. https://www.europol.europa.eu/cms/sites/default/files/documents/cyber-telecom_crime_report_2019_public.pdf
2. https://mobileecosystemforum.com/mobile-operators-and-a2p-sms-tracking-the-evolution-in-fraud/
3. https://www.gsma.com/services/fis/
4. https://www.enforcementtracker.com/