Increased federal commitment to cyber security: How secure is Switzerland?

Summary report | 16th FSS Security Talk on February 21, 2024, Swiss Cyber Security Days

As the most innovative country in the world, Switzerland is an attractive target for cyberattacks. Many companies and organizations have recognized the danger. The topic of cyber security is also a high priority for the federal government, and further important institutional and legislative changes were adopted last year. At the 16th FSS Security Talk, which took place for the first time as part of the Swiss Cyber Security Days, these changes were discussed by renowned experts such as **Martin von Muralt** (Delegate for the Swiss Security Association SVS), **Maja Riniker** (National Councilor, member of the SiK-N and the Parliamentary Group Cyber), **Tobias Schoch** (Chief Security Officer, AXA Switzerland), **Gerhard Andrey** (National Councilor, member of the SiK-N and the Parliamentary Group Cyber) and **Florian Schütz** (Director of the Federal Office for Cyber Security).

What impact can we expect the creation of the new State Secretariat for Security Policy SEPOS and the Federal Office for Cybersecurity BACS to have on Switzerland's cybersecurity architecture? To what extent does the Information Security Act change the minimum requirements for federal information security? To what extent is the private sector responsible for increasing cyber resilience?

These and other important questions were discussed in the panel discussion, which was moderated by **Fredy Müller**, Managing Director of FORUM SICHERHEIT SCHWEIZ. He welcomed the audience and explained that the aim of the discussion was to promote understanding of the latest changes in Switzerland's cyber security architecture.

Diskussion
Discussion en panel
Martin von Muralt
Delegierter für den Sicherheitsverbund Schweiz SVS
Maja Riniker
Nationalrätin (FDP, AG), Mitglied der Parlamentarischen Gruppe Cyber
Tobias Schoch
Chief Security Officer, AXA Schweiz
Gerhard Andrey
Nationalrat (Grüne, FR), Mitglied der Parlamentarischen Gruppe Cy
Florian Schütz
Direktor Bundesamt für Cybersicherheit
21. Februar 2024
16. FSS Security Talk | Verstärktes Engage

A concerning record

After this brief welcome, Fredy Müller introduced the topic by pointing out that at the beginning of November last year, Florian Schütz's organization, then still the National Cyber Security Centre NCSC, registered 2,000 reported cyber incidents in one week, which was a new record. He also pointed out that these were only the reported incidents and that there also was a large number of unreported incidents. He turned to the two politicians and wanted to know whether they were surprised by this figure.

Maja Riniker stated that she was hardly surprised, but at the same time greatly appreciated the existence of the Federal Office for Cyber Security, which can be contacted with questions on cyber issues and also acts as a central reporting office. The Security Policy Committee is also constantly confronted with the topic of cyber security, as well as security as a whole. Unfortunately, the bitter reality is that current geopolitical developments mean that people are no longer surprised so quickly.

Gerhard Andrey is also not surprised by the figure mentioned, but he believes that there are always two messages, which is why the whole thing needs to be looked at in a more nuanced way. On the one hand, the number of cyber incidents is indeed steadily increasing, but on the other hand, they are also being reported more and more consistently. As an optimist, he has the impression that some things will improve. For example, a number of legislative projects have already been launched and are now in force. However, he also has to admit that there are still areas where the situation is appalling. So there is hope and disillusionment at the same time.

Not a revolution but an evolution

Following these two answers, the moderator noted that important institutional changes in the area of cybersecurity have come into force since the beginning of 2024. He then asked the new Director of the Federal Office for Cybersecurity, **Florian Schütz**, why this new federal office was needed and what would improve with its creation.

He replied that the Federal Council had discussed the organizational form of the then NCSC in August 2022 and had come to the conclusion that it made sense to create a new federal office. This was because the NCSC did not quite fit into the regulatory landscape, the employees were subordinate to the FDF General Secretariat, but Florian Schütz, as the then Delegate for Cyber Security, was directly reporting to the Federal Council, which led to certain areas of tension. Accordingly, different organizational forms were discussed. The chosen organizational form gave the Federal Council the opportunity to control the Federal Office directly and the former NCSC also gained importance as a federal office. For these reasons, the NCSC was transferred to a Federal Office for Cybersecurity within the DDPS on 1.1.2024 in order to make better use of potential and existing synergies. The first synergies have already been manifested at the beginning of the year, and further synergies will be analyzed in the current year. When asked what should be improved, Florian Schütz replied that BACS is not a revolution, but an evolution. Existing work will be continued, but at the same time the processes should be optimized to be faster and more efficient. At the same time, the cantons and municipalities need to analyze which additional services the federal government should provide. The BACS would also receive requirements from the economy and the population, but these would have to be defined and dealt with accordingly via politics.

Fredy Müller then turned to Maja Riniker and wanted to know whether the Security Policy Committee had been informed about this structural change.

Maja Riniker believes that the importance of the topic has been correctly addressed with the creation of the federal office. This is because cyber security is not only addressed in isolation, as the new State Secretariat for Security Policy also deals with general security policy. Accordingly, the importance has been recognized and resources have been correctly allocated. In addition, the consolidation under a new title will lead to an improved and changed perception internationally, which is of immense importance, especially for topics that do not stop at a cantonal or national border, as exchange and visibility are key.

Lack of clarity in the areas of responsibility of the new administrative units

The moderator summarized that the State Secretariat for Security Policy, SEPOS, and the Federal Office for Cybersecurity, BACS, had been newly created, thus creating an adapted security architecture in the cyber area. He also wanted to know from **Gerhard Andrey** how important it was that these structures had been created, both internally and externally.

The latter welcomed the creation of the federal office and recalled the corresponding announcement by the then Federal Councilor Ueli Mauer. He also mentioned that he had already raised the question of whether such a federal office should be created in parliament before the official announcement. However, the Federal Council had reacted very cautiously at the time. Even though the BACS now exists, he still sees some major question marks, particularly with regard to the organization. Because no sooner had the BACS been founded than a new state secretariat was created, with which there would be overlaps in the area of activity. There is therefore a need for more clarity. He added that, in general, something old has to work properly before something new is started. The current situation is that the Federal Council is still figuring out the exact implementation and organization of the Federal Office, even though it was already operational.

The moderator then asked **Florian Schütz** whether there were any conflicts of competence or a confusion of information between SEPOS, the Cyber Command and the BACS and how this Gordian knot could be untied.

The interviewee replied that in his opinion this was not a Gordian knot. He was of the opinion that a great deal of clarity had been created by working with the army over the past four and a half years. This is because the army is responsible for army tasks, while civilian tasks fall to the police authorities at cantonal or federal level, whereby they work closely together and support each other. The State Secretariat primarily deals with strategic security policy issues, of which cyber is only one part. There is a certain amount of overlap, which should and must be delineated in the future. Due to the relocation of the specialist unit for information security and the establishment of operational security and personal security checks in SEPOS, there is now a focus on internal security. This allows the BACS to focus more on its core tasks - implementing the national cyber strategy and improving the protection of the economy, education, society and authorities. As a public authority, the Confederation remains an important user of BACS services and benefits from direct protection - both preventive and reactive. Finally, Florian Schütz added that there are always different models with which such a cooperation can be organized. Therefore, the current model must be further elaborated and reviewed at the end of the year to see whether it works.

The moderator followed up and wanted to know what the specialist unit for information security was and what its location at SEPOS meant.

Florian Schütz replied that before the ISG came into force, the instruments available to the Confederation were limited. At that time, there were two different bodies: the IT security guidelines in the NCSC and the information protection guidelines in the DDPS General Secretariat. This separation was difficult to implement and both could only affect the Confederation. With the new ISG, the regulations will apply to everyone who processes federal data. Accordingly, the Confederation will also receive audit rights which it could not make use of before. One example of this is third-party supply chain management.

The Swiss Security Association - A unique entity

Fredy Müller moved on to a new topic and asked **Martin von Muralt**, the delegate of the Swiss Security Association (SVS), to explain to the audience what its exact remit is.

First of all, he clarified that he was not the delegate of the Federal Council, but of the Confederation and the cantons. This was important in order to understand exactly what his mandate entailed. The SVS is a unique organization that only makes sense in a federal state. The SVS is responsible for good offices between the three levels of government within Switzerland in the area of security. Cyber plays an important role in this but is not the only part. The strength of the SVS lies in the fact that it operates on a parity basis and the municipalities are also involved in the respective security-related topics. The association is agile and takes on current topics that are of strategic and political importance. Cyber, for example, would not have been an issue for the SVS ten years ago, but has since developed into a central element that will continue to be important in the future. The SVS is a mechanism that ensures that the correct framework conditions are created in the Confederation and that the Confederation, cantons and municipalities talk to each other about security-related issues. Consensus is sought, areas in need of action are identified and catalogs of measures and strategies are developed. The SVS is currently active in the areas of extremism and radicalism, human trafficking, cyber and crisis management, as well as future topics that are already in the pipeline. The alliance is a construct that enables dialogue between the levels of government in the security sector in an agile and topic-related manner. The issues are different today than they will be in five to ten years' time. In the cyber area, the SVS has two roles. The first arose around five years ago when the national cyber strategy was introduced and the existing cantonal strategies had to be adapted. The development of the national cyber strategy NCS by the NCSC was carried out in close cooperation with the cantons. A cyber security specialist group with all partners involved at federal, cantonal and municipal level is planned for the implementation of the NCS, so that the issues of self-empowerment, resilience and incident management can be addressed and dealt with jointly.

Fredy Müller was visibly astonished by the SVS's wealth of tasks and wanted to know from **Martin von Muralt** how many employees he had at his disposal and how many he could rely on for support in the working groups.

He reiterated that the SVS is a mechanism or label that involves equal and neutral participation. Accordingly, it has no resources or decision-making powers of its own, apart from its own office. For this reason, the SVS staff is rather small, with only 5.4 FTEs (full-time equivalents). However, there are six members at federal level and a further six at cantonal level, who are ultimately responsible for implementation. The SVS is only responsible for coordination, through which the need for action and catalogs of measures are identified and strategies are developed. Implementation is then the responsibility of the respective partners. If necessary, the SVS could carry out strategic monitoring afterwards and support the whole process. However, it is strategically and politically affiliated and therefore cannot directly draw on human resources.

Coordination between the different levels of government

The presenter wanted to find out more about the coordination between the three levels of government and asked what the response to an explosive cyber incident would look like.

Florian Schütz was of the opinion that the approach to an incident is relatively simple. Incidents attract a lot of attention because they are exciting to listen to and have a certain drama to them. The handling is time-consuming and finding weak points can be challenging. However, it is much more difficult to build secure systems. We should focus more on creating systems that prevent incidents. This is the much more exciting aspect. With regard to a cyberattack on a canton, he replied that if only one canton was affected, it would take action itself. If it was not in a position to do so, it would contact the BACS and receive appropriate support. It would be more complicated if several cantons were affected and the incidents had a far-reaching impact, as was the case with Xplain, for example. At that time, a large number of cantons and companies were affected. Coordination in this incident had not yet worked optimally. Accordingly, it became clear that a certain set of instruments was missing, for example how incidents were to be classified and coordinated in the same way across government levels and how strategic issues were to be dealt with. The BACS is therefore working together with the KDK, KKJPD, the various federal agencies, the SVS and the political sphere so that these processes can be standardized without compromising the autonomy of the federal system.

Fredy Müller went on to ask how such cooperation takes place and whether there is a regular exchange.

Schütz went on to say that we need to move away from the idea of a room in which meetings on the current situation are held regularly every few hours. This does not work in practice, especially in incident management. Today, everything is done via telephone, encrypted messaging services and digital platforms, and the BACS also operates a digital room for critical infrastructures and the cantons. In addition, coordination meetings are held on an ad hoc basis. The committees that exist in Switzerland, including at cantonal level, are important for preparation.

Fredy Müller then asked **Martin von Muralt** about awareness of increased cyber resilience to cyberattacks in the cantons and municipalities.

He is of the opinion that the awareness is becoming ever greater. Additionally he commented that the exchange in the area of cyber security between the Confederation and the cantons should take place via the platforms of the SVS. This had recently been made possible. He had been arguing for years that Florian Schütz should become a member of the SVS operational platform, which had now been approved. We are now in a pilot phase. The municipalities are also represented on the SVS, as can be seen from the mandatory obligation to report incidents on critical infrastructures. The municipalities were asked whether they felt affected by this issue and whether the reporting obligation was perceived differently depending on the size of the municipality. However, all municipalities welcomed equal treatment. This goes to show that even small municipalities are aware of cyber risks. He was pleasantly surprised that the small municipalities without their own IT capabilities, i.e. those that have outsourced their IT to private sector companies, are aware of the risk. However, the challenges in a federal state with different structures remain great. Zurich cannot be equated and compared with a small municipality.

Maja Rinker added that this empowerment of individuals, companies or municipalities, the lowest level of government, is very important. Attacks or abuses could occur at any time and it is therefore crucial that people know how to deal with them. An example from the Security Policy Commission illustrates this point. It was about the fact that asylum applications can also be submitted to the municipalities, which are organized differently. However, all municipalities are confronted with applications that are made using a forged passport. A special device is needed to detect this, whereby the decisive factor is not the price, but the availability of these devices and trained personnel. She therefore believes that the SVS fulfills a very valuable task. She also shares Florian Schütz's opinion that the system should prevent attacks and that the state should offer more protection.

A better overview of current cyber threats thanks to the new reporting obligation for critical infrastructures

With the revision of the new Information Security Act, operators of critical infrastructures must report cyberattacks that affect the system. Fredy Müller wanted to know from the Director of the BACS what this would improve for the general public.

Florian Schütz explained that it has been possible for all critical infrastructures in Switzerland to voluntarily report cyber incidents since 2004. Such reports had increased, but some companies and organizations had taken reporting more seriously than others. The federal government and parliament were therefore of the opinion that a reporting obligation was needed to create parity, as correct statistics were needed. Because taxpayers' money is being invested, the statistics must transparently show the biggest problem areas. Unfortunately, cyber is a very marketable issue, which became evident during last year's denial of service attacks. Newspapers were suddenly full of experts propagating the big Russian attack. In reality, it was a DDoS attack, which would not even have had an impact on gross domestic product. In fact, the attackers were only successful because they were given a larger platform and therefore a greater reach. At the same time, there was a serious problem with the hacker attack on Xplain. Due to the reporting obligation, the BACS is obliged to help operators of critical infrastructure in the event of an attack. So far, this has been done on a voluntary basis. This will be a challenge in the future, as a 30% increase in incidents means more work. The BACS currently receives information about a malware infection every forty minutes, which affects not only critical infrastructures but all companies. Schütz is of the opinion that the BACS should also offer help for non-critical infrastructures - which are not subject to a reporting obligation - in the future. With regard to critical infrastructures, the law defines a maximum threshold as to who is obliged to report. The BACS is in the process of drafting the ordinance and is planning a consultation this year, which will define the effective threshold.

The interdependence of data

Due to the attack by the Chinese hacker group "Volt Typhoon" on critical infrastructure in the USA, the moderator asked whether there was a list of critical infrastructure in Switzerland.

Florian Schütz answered in the affirmative and referred to the Federal Office for Civil Protection, which is responsible for this list. He believes that it is more important to ask the question of whether it is expedient to only ever talk about critical infrastructures. After all, cyber security affects all companies. In the context of the reporting obligation, the restriction to critical infrastructures makes sense, as there is also a clear definition of critical infrastructures in the ISG. One of the tasks of the Federal Office for Cybersecurity is to support operators of critical infrastructure in the event of an incident. However, if an SME gets into difficulties, they cannot be helped directly by the BACS; to exaggerate somewhat, the SMEs are left to their own devices. This distinction between critical and non-critical infrastructure is therefore somewhat problematic. In addition, around 75% of Swiss companies generate less than half a million CHF in turnover per year. Depending on the industry, this leaves a budget for cyber security of a few thousand Swiss francs. This could possibly be used to buy an antivirus license. If all pharmacies in Switzerland were to fall victim to a widespread ransomware attack that exploited a vulnerability in the pharmacy system, this would be a systemic problem, even if an individual pharmacy was not necessarily systemically relevant. It is therefore important that the BACS can also help non-critical infrastructures where appropriate.

Gerhard Andrey added that he would also like to question the distinction between critical and non-critical infrastructure. At the same time, he pointed out the danger that certain companies would accept a business interruption due to a cyberattack too easily. The problem with this perspective is that in the vast majority of incidents, others are also affected. He used the example of a doctor's surgery where several thousand patient files are stolen, which ultimately has an impact on the people affected, as their personal data has been misappropriated and could be further misused. In his opinion, it is precisely this kind of affectedness of others that is often taken too lightly. There have also been incidents like this at CH-Media or NZZ, where one door suddenly opened another one. It is crucial that the importance of the stolen data is taken into account and that it is not viewed as something isolated. As already mentioned, he had the impression that some companies were somewhat careless in the way they handled such cases.

The moderator asked the panel what the consequences of stolen data would be.

According to **Florian Schütz,** the consequences can be very diverse. They can range from identity theft to improving phishing, etc. In general, however, what goes public remains public and can no longer be undone. Finally, there are various instruments to combat data theft. On the one hand, however, the law enforcement authorities must continue to be empowered to eliminate such groups. Shortly before this panel discussion, it was reported in the news that an international strike against Lockbit had been successful – with Swiss involvement. At this point, it should be noted that the Swiss law enforcement authorities are active and efficient. On the other hand, the whole issue needs to be looked at more broadly. In addition to the direct prosecution of criminals and the seizure of their infrastructure, there are other instruments. Criminals want to make money. The more difficult you make it for the criminals and disrupt financial flows, the less profitable it becomes for the criminals. Switzerland is also relatively active here in international dialog, for example together with Singapore, in the area of anti-money laundering and counterterrorism financing mechanisms for VSOPs and cryptocurrencies. Switzerland is also represented in international bodies, such as the Counter Ransomware Initiative, which was initiated by the USA and comprises around 50 countries. Such cases must be closely examined and the flow of money must also be tracked. More than 95% of all cyber incidents are of criminal nature, which is good news for all viewers, because you don't have to be the best in cyber defense, but simply better than the others, as criminals always choose the path of least resistance.

Gerhard Andrey
Nationalrat (Grüne, FR), Mitglied der Parlamentarischen Gruppe Cyber
Florian Schütz
Direktor Bundesamt für Cybersicherheit
ersicherheit: W
e Schweiz?
2

Exchange between the private sector and the federal government

With this , Fredy Müller turned to the representative of the private sector on the panel, **Tobias Schoch**, and wanted to know whether an insurance company like AXA was also part of the critical infrastructure.

He confirmed that AXA is a critical infrastructure. As Florian Schütz had already mentioned in advance, there was a definition of critical infrastructure and insurance was part of it. It is a sector that requires extensive protection. AXA itself is also affected by this and heavily regulated by FINMA. It therefore has clear requirements that must be met.

The moderator also wanted to know from **Tobias Schoch** whether there was some kind of committee or body through which an exchange between the private sector and the federal government took place.

He said that the exchange and cooperation with the federal government is a key element today. He has 20 years of experience in the IT security sector and was therefore able to observe that the situation back then was very different to today. The topic has gained momentum and today this opportunity for cooperation is being used more and more. One illustrative example is the weekly BACS call on Wednesday mornings, where operators of critical infrastructures can dial in for around fifteen minutes and receive information about the latest attacks and which companies have been affected. These calls are also very valuable for AXA, as they provide information that was not available before, especially not at the speed that is available today. In this respect, digitalization has also helped greatly in making such an exchange possible at all.

Fredy Müller wanted to know from **Florian Schütz** what the response to this was.

He replied that the feedback was very positive, but he had the impression that there was a broadly shared interest in even more opportunities for exchange. In addition to these calls, there was mainly a desire for information that could be accessed asynchronously. BACS is already working on this and hopes to be able to meet these requests as soon as possible.

Fredy Müller then turned to the private sector again and wanted to know how a large company like AXA deals with cyberattacks.

Tobias Schoch does not see AXA in a special position; they are confronted with the same problems that other larger companies have to deal with. AXA may have the advantage of having recognized the issue very early on. He started at AXA five years ago and had previously worked in the banking sector. In this sector, massive investments were generally made in IT security. In the case of AXA, the head office is in Paris and clear requirements are sent from there to the branch in Switzerland. There is not much room for negotiation, because ultimately it is always about protecting the whole of AXA worldwide. However, his team of around 30 people is responsible for Switzerland. Of the approximately 150,000 employees worldwide, some focus on security and defense against cyberattacks. There are different types of attacks and not every "ping" counts as such. Of course, there are also internal attacks or incidents when data is mistakenly sent out when it shouldn't be. This is where data protection plays a greater role.

An appeal to the personal responsibility of SMEs

The moderator took this idea further and referred to Florian Schütz's statement that 75% of Swiss SMEs have an annual turnover of less than CHF 500,000 and wanted to know from the politicians whether this fact did not worry them.

Gerhard Andrey responds with a figurative analogy. Many SMEs leave their doors open over the weekend. You have to appeal to them so that these companies take their responsibilities seriously. He would increase the pressure on these weak points because they potentially affect other players. In his company, too, he has seen cases where service providers have had problems that have had a negative impact on his company. In the past, he has sent out 130 registered letters on the subject of "close the door". These are basics and everyone is responsible for their own safety. He misses this delta or the awareness that others could also be affected and that you have to be more careful yourself. Politicians need to be tougher in this respect. He therefore sees a solution in directors' and officers' liability. As a Board of Directors, for example, you have non-delegable tasks, such as the responsibility to ensure that there is an appropriate financial governance. He is also of the opinion that in the 21st century, data governance is a non-delegable task. It is clear that everyone is responsible for their own security, but also for the supply chain, the customers, and something needs to be done about this.

Fredy Müller turned to Maja Riniker with the question of whether such proposals are also discussed in the SiK-N, the Security Policy Committee of the National Council. He also wanted to know what the tenor was there and whether it was all the responsibility of SMEs if data was wrongfully released.

Maja Riniker posed the rhetorical question of what the role of politics actually is. According to her, it is primarily responsible for external security, where the army is discussed, but also for internal security, which includes important tasks. It is about money laundering, crime, the federal police, etc. She is of the opinion that every entrepreneur is responsible for the first steps and must also bear the risks. Riniker, as an FDP member and supporter of entrepreneurship, admires every entrepreneur, but the state is not responsible for insuring and supporting all individuals and companies. The security policy committee would not be discussing the issue at this level, nor would it be appropriate in her opinion. Nevertheless, she recognizes it as a relevant discussion, and in particular it should be clarified from what size a company needs cyber insurance. The next step would then be to clarify who is in charge of this. "If the entrepreneur doesn't take care of it, what are the sanctions?" asked Maja Riniker. There would be fines and prosecutions. Switzerland is not yet very advanced in punishing very serious offenses. More resources could be invested in proper prosecution. However, until more resources are invested in this area, Riniker believes that it is not right to prosecute every "SME" if they have not taken out the right cyber insurance.

As Martin von Muralt often has to deal with the cantons and municipalities, Fredy Müller approached him on the subject of personal responsibility and SMEs.

Martin von Muralt did not comment on SMEs, but referred to personal responsibility and the subsidiarity criterion, which are in Switzerland's DNA. The municipalities, cantons and population were responsible for themselves. The federal government could not rush to aid after every attack. We must ensure that the cantons and municipalities are independent, which they already largely are. But municipalities are like SMEs, they do not have unlimited resources. It would therefore make sense to consider how synergies and best practices can be used and how exchanges between cantons can be promoted, whether for self-empowerment or incident management. Mr. von Muralt agreed with Maja Riniker, that personal responsibility also applies to SMEs at state level. The questions remained: when can a municipality and a canton expect support from the federal government? When will support come from the BACS? In his opinion, these were things that still needed to be clarified.

Florian Schütz also referred to the security perspective and economics. Ultimately, the question is "can I buy a service on the market and do I know what I have bought?" Cyber is a noisy market and it is often difficult to see what is actually being purchased. The BACS deals with cases where those affected would not have suffered any incidents if they had been with a different internet service provider. As it is, they have suffered damages in the high tens of millions. However, the BACS cannot give an assessment of the various providers, as this would distort competition. At the same time, it would be the responsibility of entrepreneurs to ask themselves "what do I get from this contract and what do I allow on the market at all?" What role do consumer protection magazines play in this? For example, if you buy a teddy bear with toxic dye and this is discovered, it would have to be taken off the market. At best, there would also be claims for damages. If, on the other hand, an IT product is sold on the market that is full of vulnerabilities and transfers data abroad, there would be no consequences. The manufacturer could continue to sell the product. Mr. Schütz is not of the opinion that we need to take a regulatory approach here, nor that regulation is always the right instrument. But economic incentives, good quality products and a clean process are needed to address these issues. Every product has weaknesses when it comes onto the market, but these need to be taken seriously and consumers need to realize what they are spending their money on.

Tobias Schoch followed up and praised the example of the comparison with other companies. AXA is doing the same. The aim is to be among the top 25% in the banking and insurance sector. That is a good level in the relevant area. The Board of Directors had also approved the target so that enough could be invested to reach the 25%. AXA would be compared with 37 banks and insurance companies and would undergo an assessment. In the SME sector, it is very relevant how much "awareness" there is among management on the topic. This awareness is often surprisingly low. In such cases it doesn't take long for something to happen. Mr. Schoch was shocked at how often this is handled carelessly.

Raising awareness and demystification

Fredy Müller asked Maja Riniker about the preliminary discussion in which she had spoken about raising awareness and demystification as well as her daughters, who were already made aware of this at school.

Maja Riniker was convinced that people should no longer be ashamed if a mistake is made or an attack occurs. In such cases, the Federal Office for Cyber Security offers a point of contact. She is of the opinion that people should be confronted with such issues at an early age. Her two teenage daughters are already being made aware of this at school. She also spoke to a good friend who was CEO of a large company and which had suffered a cyberattack last year. The friend had spoken about it in the media and said that without a good insurance company, which had provided immediate liquidity, she would not have been able to get new hardware within three days. People should be allowed to talk about it and should no longer be ashamed. There needs to be a destigmatization. Maja Riniker believes that attacks are part of everyday life and we should be able to learn from them.

Gerhard Andrey highlighted this point of view. He referred Riniker to a panel at the Industry Day 2023, where both has been present. He was impressed by how some CEOs had stood up and told what it had been like to be a victim of such attacks, what their personal responsibility was and where negligence may have entered the picture. This demystification of such incidents was also essential in Andrey's eyes. He drew a connection to the Information and Security Act (ISG), where he would have liked to have seen an extension. In his opinion, vulnerabilities that were not yet known should also have been reported to the former NCSC (National Center for Cyber Security), now the BACS. The National Council would have listened to his concerns at the beginning, but the industry was not yet ready.

Fredy Müller then asked **Gerhard Andrey** about whistle-blowing.

Andrey denied talking about whistle-blowing, he was rather referring to Heartbleed or Lockbit (two specific weak spots) in his remarks. If a gap were to occur in a critical infrastructure and someone were to notice it, he would have liked there to be an obligation to report it to the BACS. But they hadn't gotten that far yet. Andrey was sure that it was only a matter of time before this obligation came. At the end of the day, the realization that "if there's a fire at my place, there could be a fire at yours" was very helpful. This train of thought should be the goal.

Fredy Müller turned to Florian Schütz and asked whether SMEs could also dial in to the weekly calls.

Florian Schütz denied that non-critical companies can participate. At the moment, the calls are limited to critical infrastructures. However, there are of course also SMEs that are considered critical infrastructure. However, there are plans to open this up, but it is important to consider whether the current form still makes sense. For example, it would be useless for a municipality to learn about the major international attack vectors if it cannot handle the information. This would have to be managed on a step-by-step and needs-based basis.

Fredy Müller gave the floor to **Tobias Schoch**. AXA is a global company that invests a lot, he said. High investments cost AXA less than if it had to pay a ransom. Switzerland is a highly innovative country. This is probably why awareness in Switzerland is higher compared to other countries. Fredy Müller wanted to know whether AXA Switzerland was more affected by attacks than other countries.

According to Schoch, this is not the case. Switzerland has been the focus of attention at certain events, such as the WEF, where DDoS attacks have taken place. If you look at the world order today, there has been a sharp increase in cyberattacks, partly due to the war in Ukraine, which has now been going on for two years. Switzerland is also in the spotlight in this respect, but not more so than other countries. Schoch sees a prejudice in the fact that attackers assume that there is a lot of money to be extorted in Switzerland. As the largest insurance company, AXA is probably more in the focus of such attacks than smaller insurance companies due to the amount of money involved.

Security network exercise 2025

In conclusion, Fredy Müller asked Martin von Muralt to share some information on the next security exercise "strategic command and control exercise 25" and wanted to know whether awareness-raising and prevention against such attacks would be practiced.

Martin von Muralt confirmed that it was about raising awareness, but not about prevention, as it is crisis management and prevention takes place in advance. It was an integrated exercise, as the security network exercises and the strategic command exercises were being brought together. For the first time in Switzerland, the Federal Council will be exercising together with the cantonal and government councils, critical infrastructures and with the involvement of the scientific community. The topic is well-known and relatively broad: "hybrid threat to Switzerland". There are three main objectives for this exercise. Firstly, the aim is to test how the entry into the crisis works, secondly, the resilience, and thirdly, communication coordination. Cyber includes cyber security, resilience, incident management, but also cyber warfare. The latter, with reference to communication, often stems from disinformation. In response to this, we need to ask ourselves "how do we cope, how do we react, how do we coordinate when foreign disinformation campaigns are used?" This will be the focus of this exercise.

Insights for the audience

To conclude, Fredy Müller wanted to know from everyone what the most important findings were for the audience in the area of cybersecurity.

For **Florian Schütz,** the whole issue was one that transcended national, economic and social levels. Attack and defense should not be viewed in isolation, as that would be too short-sighted. Good strategic approaches and implementations would create added value while taking social and economic aspects into account.

Gerhard Andrey agreed with this and added another aspect. He was also a member of the Finance and Security Committee. Finding a balance between the available funds and the security and defense needs is not easy, he said. He expressed criticism of the amounts transferred, which flow into the army and not into defense. In his opinion, the means and not necessarily the ends were getting the money. Many things are relevant to security, not just the army, and he wants to ensure that a good balance is found. After all, not all risks that are already painful today and will increase in the future can be managed with sheet metal, steel and cannons. And this is where we need to make sure that we don't lose our balance and slip into militarism.

According to **Tobias Schoch**, it is not that difficult for the private sector to maintain the immediately necessary protection. This includes multi-factor authentication, encryption and immutable backups for ransomware attacks, which should be built in. These are core elements that need to be implemented. He was of the opinion that SMEs are also well positioned with these core elements. They do not offer 100% protection, but it is a step forward. If a little investment was made here, Switzerland as a whole would grow in this area.

Martin von Muralt addressed the complexity of the entire topic. However, this complexity is a given. There is cyber defense, law enforcement and security. In addition, responsibility is spread across the three levels of government, which also increases the need for coordination. However, it also brings advantages. Thanks to this federalist system, new ideas and small laboratories are emerging everywhere. This has a creative character and can generate good ideas and goal-oriented cooperation. The second is the proximity to the population, which is provided by the cantons and municipalities. There is great diversity here, but also a risk due to the various providers in the cyber sector. Nevertheless, it also offers protection, as not everything is centralized in one place and therefore

Switzerland cannot be attacked at one point. If we want to talk about infrastructure resilience, the various resources must be coordinated, processes and minimum standards must be in place, and that is the challenge.

Maja Riniker concluded with some reassurance. In politics, money is not only spent on "steel and artillery". There is a cyber battalion, a cyber RS is being carried out and research is also being conducted in this area. A lot of money is also being invested in this area. The Security Policy Committee is aware that the topic of cyber is very important. The Commission may not be made up of the cracks, such as the audience at the Swiss Cyber Security Days, but the topic is always on the agenda, be it in exchange with the national supply, when the Federal Office for Civil Protection, the Director of the Federal Office for Cyber Security, Mr. Schütz, or the Director of fedpol, Ms. della Valle, are in the Commission. Today, the audience can take away the certainty that politicians are confronted with the issue and are certainly taking it seriously. There will probably never be complete protection. But the awareness is there.

The inquiries showed that the audience was very interested

Fredy Müller thanked the panel guests and gives the floor to the audience.

One member of the audience asked how the reporting obligation mentioned could be implemented or monitored in the event of cyberattacks.

Florian Schütz responded to this with the corresponding procedure. There will be a notification form for the implementation. Depending on the sector, there are already reporting obligations to regulators, as is already the case in the financial sector, for example. Work is currently underway to ensure that, if possible, there will only be one reporting office, which will distribute the report in a second step. This should be very low-threshold and it is not necessary to go into detail. We do not want to impose any additional work. If something is not reported and the BACS learns about it, the company can be warned and informed that a reportable event has occurred, which must be reported subsequently. If the organization concerned fails to comply with the reporting obligation after repeated requests, a fine could be imposed.

One audience member shared a suggestion with the panelists. The panel had talked about companies taking responsibility for their own actions. In this regard, he wanted to refer to the financial industry and the Federal Council's Brunetti Advisory Council on the future of the financial center, which was the trigger for the militia system and cooperation between the federal government and industry. In his opinion, the Confederation or politics can sometimes be the spark that ignites the militia.

Gerhard Andrey could support this. He addressed an interpellation he had submitted, in which he asked the Federal Council whether it would be possible to learn from examples of best practice. He was also on the Board of Directors of a bank, the Alternative Bank, and therefore knew a little about how things were handled. FINMA had already issued circulars years ago, which were written in a sharp tone. As a result, there were probably fewer cases of attacks in the financial industry, but it should be noted that the industry had already made sharp transactions early on. In his interpellation, he had asked the Federal Council whether there were already supervisory bodies in industries that could take over supervision for the respective areas in a similar way to FINMA. He could no longer give the Federal Council's exact answer. But he was clearly in favor of building on good examples.

Fredy Müller then closed the plenary session and thanked the audience for their attention and Jürg Walpen as well as Nicolas Mayencourt for organizing the Swiss Cyber Security Days.