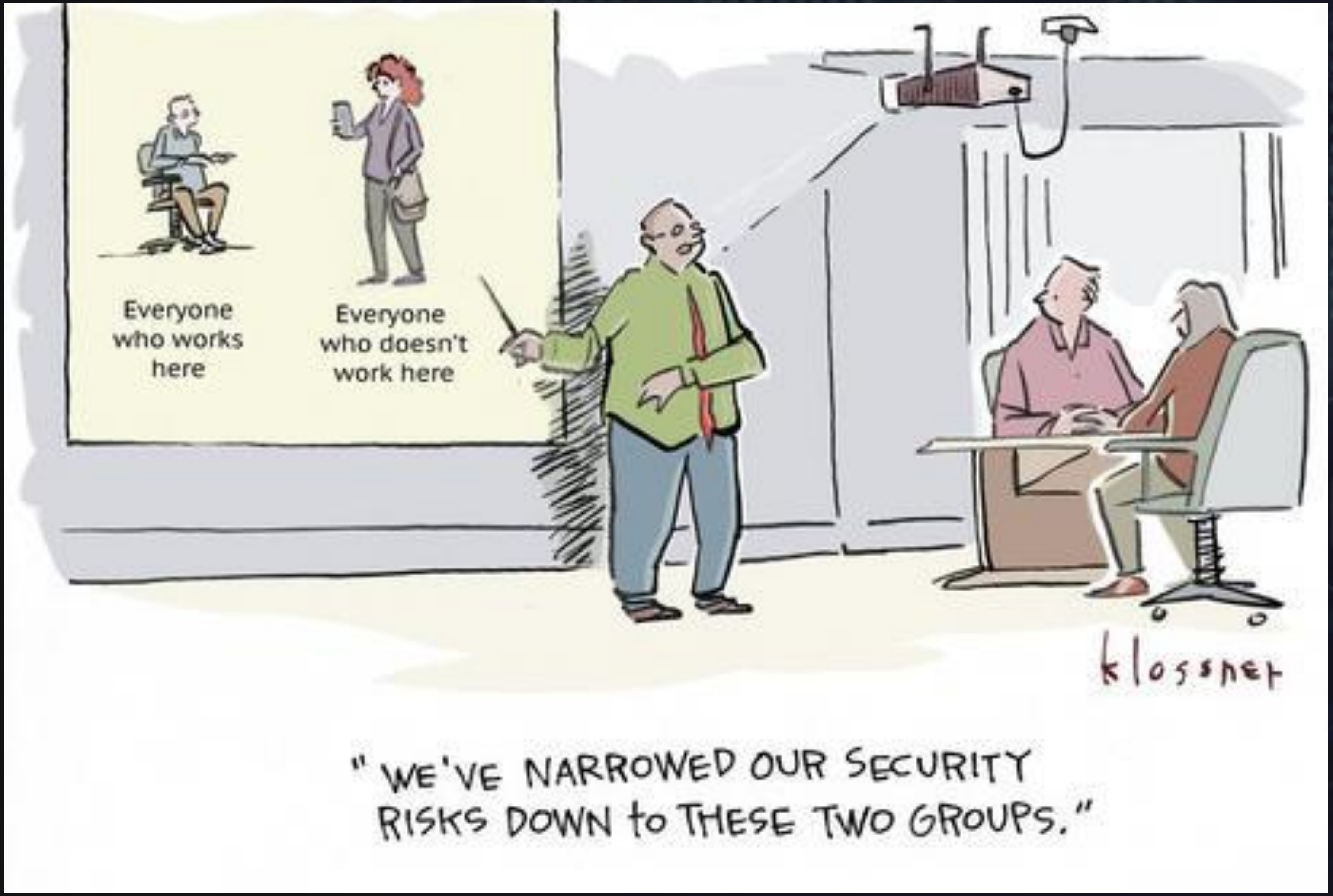
A usual day of a cybersecurity manager ...

Rastislav Janota
director

SK CERT

NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI


Everyone who works here
Everyone who doesn't work here
klossner
" WE'VE NARROWED OUR SECURITY RISKS DOWN to THESE TWO GROUPS."

The issue of cybersecurity should concerns everyone.

Each one of us is responsible for our own data, services and devices.

MY COMPANY

My company/organization has started to carry out the Act on Cybersecurity

- It designated a cybersecurity manager (actually it's me ☺ and it was 6 months ago), who
  - may submit proposals and report information in the field of cybersecurity directly to the managing director as well as the managing board,
  - ensures the implementation of security measures in the system of cybersecurity management,
  - is independent of the management of the operations and development of information technology services, and
  - meets the knowledge standards required for the position of a cybersecurity manager pursuant to a special regulation (here we did as best we could; a special regulation does not exist yet, but I'm a certified internal auditor according to 27001).
- My task assigned by the managing board is to ensure that our company's obligations under the Act on Cybersecurity are met and will be met.
- For my main co-workers big boss appointed: a head of operations, head of IT, head of personnel and our lawyer.
- As one of my tasks was also to introduce a development plan of colleagues in the field of cybersecurity, so that I wouldn't be alone in it.

CYBERSECURITY MANAGER

- **As a cybersecurity manager, over the last 6 months, I focused on**
  - creating the cybersecurity strategy in the organisation
  - information classification and categorization of networks and information systems in then organisation
  - setting the minimum requirements for security measures that depend on categorization of networks and information systems (according to law if any and based on well defined standards like ISO27001, NIST, COBIT)
  - Typically different requirements to different categories of systems

When creating the documents I co-operated not only with colleagues from various departments of our company but also with an external certified cybersecurity auditor/consultant who advised us how to do the best.

We came to conclusion (when trying to find someone who would give us advice) that there are many companies on the market today claiming that they are able to help us, but in fact they do not have the knowledge and/or experience to do so. Therefore, we decided to co-operate only with a certified cybersecurity auditor/consultant, who has a duly validated qualification in this field.

HOW OUR PREPARATIONS LOOKED LIKE

- We have been concentrating on
  - information security organization,
  - management of assets, threats and risks,
  - personnel security,
  - management of supplier services, acquisition, development and maintenance of information systems,
  - technical vulnerabilities of the systems and equipment,
  - management of network and information system security,
  - operational management,
  - access management,
  - cryptographic measures,
  - cybersecurity incidents handling,
  - monitoring, testing of security and security audits,
  - physical security and security of environment,
  - process continuity management.

HOW OUR PREPARATIONS LOOKED LIKE

- Besides the document preparation we started with training preparation – we know that this part is the most difficult one because the results can be expected much later – we have been searching for external professional Partner in this field with whom we have prepared a training schedule for all our employees (awareness training – for administration, finance, sales, marketing and other computer users in the company); the Partner carried out the first round of training for us and thus prepared our future internal trainers for this field.

- Our IT deployed better detection tools – all new things were from Open Source category – as the Financial Director carefully guards the budget. But in the field of detection it doesn't affect the quality – we just had to do a lot of things ourselves – learn something or experiment a bit. But experts from the national CSIRT were a big help with their practical recommendations.

- We began with hardening according to policies – updates, firewalls on servers, centralized log management. Step by step, we try to decommission obsolete operating systems. In order to know/detect if our data has become easy prey, we ordered external penetrations tests for our own software and important network segments.

HOW OUR PREPARATIONS LOOKED LIKE

- We also found other external partner – this time it is SOC/CSIRT. They would collect results from detectors on our security perimeter (logs from our IDS/IPS, firewalls, routers, DNS servers, WAF and also e-mail and web servers), logs are evaluated and the outcomes of evaluation are sent back to us for further handling. This helped us a lot because evaluation to this extent is very difficult for us in terms of finance and personnel...
- It was smart to choose only from internationally recognized CSIRTs – member of FIRST and/or at least accredited member of Trusted Introducer organizations
- There is also one rule – task for external SOC/CSIRT is to pinpoint all potential problems. If we would have this role internally it may in the future lead to less efficient detection as they will realize their work is not popular in the company.
- Of course external SOC did not fully meet our need of security monitoring. We don’t have enough qualified internal staff who is important to help solving all detected problems/incidents in our infrastructure.

So today, we think that we are well prepared for critical situations, for incidents, from prevention through detection to response.

BUT WE'RE NOT DONE

- What else can we expect?
  - We have our documentation, strategy, policies and so on, but colleagues must get used to it, experience it; it must become a regular part of their work
  - And we do not forget that this documentation is a living set of materials; we ensure a process of its regular maintenance and updates, especially in the field of risk updates and evaluation of adopted measures' effectiveness
- But that's not enough...
  - people (even those trained ones) still understand cybersecurity as something just for geeks, for IT egghead colleagues
  - people from the company (sales, marketing, finance as well, and even lawyers and PR team) don't understand so far an extreme importance of the issue of cybersecurity for our core business in the company; and if we all (within our work duties) don't start to pay attention to it and deal with it, it may cause significant direct and also indirect damage to our company
- So what did we do?
  - We asked external company for the possibility of participation on their companies table-top exercise. It wasn't easy to convince our top management and the managing board members to participate in the exercise. These exercises are non-technical ones – they focus on relation of cybersecurity to business, to company's activities. A typical team is made up of people such as a head of finance, head of operations, head of sales/marketing, lawyer, someone from PR and a head of IT. So, all of them are managing board members or from the first-line below the managing board. But we did it, we participated for the first time, we liked it and agreed on repetition with a every new/different exercise scenario.

SO WHAT DOES MY DAY ACTUALLY LOOK LIKE?

On a usual day I alternately focus on

Preventive measures

- Documentation updates, evaluation of measures and as needed a risk update
- I work a lot with my colleagues – employees of the company
  - I see their regular training as one of the most important measures to reduce risks (almost every risk)
  - We know that targeted and also accidental (much more often) malicious behaviour is the cause of most incidents
  - We regularly update training materials when new methods of attacks or new forms of threats emerge
  - Training is compulsory for every new employee in the company (internal as well as external), it must be repeated at least once every two years (maybe in future once a year)
- However, we do not forget about preventive measures in IT operations – updates, penetration tests of new and updated SW and HW systems that IT is planning to deploy and so on.
- We pay particular attention (but not only) to
  - Malware, Phishing, DDoS, Ransomware, Hacking, misuse of known and also Zero-day vulnerabilities, MitM attacks, SQL injections, XSS, social engineering and many other methods.

SO WHAT DOES MY DAY ACTUALLY LOOK LIKE?

On a usual day I alternately focus on

Reactive measures

- I co-operate with SOC/CSIRT, assist them in seeking/setting rules for evaluating the events in our organization in order to minimize False Positive as well as False Negative situations.
- Together with SOC/CSIRT we regularly organize trainings of internal procedures, incident simulation and we train our colleagues to respond correctly according to the situation.

SO WHAT DOES MY DAY ACTUALLY LOOK LIKE?

On a usual day I alternately focus on

Co-operation

- We co-operate with national CSIRT and sectoral CSIRT in my country
- We actively participate in co-operation within our sectoral Centre of experience and knowledge sharing and information analysis – ISAC which is either organised in the country or in some cases (where missing locally) we tried to joint e.g. European ISAC if exist in my sector.
  - The mission of ISAC is to assist and support the operative protection and the cybersecurity response within sectoral communities. This is ensured through information sharing within the community of trusted representatives.

And all this happens in days when we're lucky and don't have to handle any incident (less or more serious)...

SECURITY MEASURES

So, where do we find the most problems in companies/organizations?

Management

- Lack of security perception
- Misconception of responsibility
- Reluctance to invest

Security professionals

- Great shortage of people
- Poor quality in general
- Weak security knowledge
- Little training

IT employees

- Vague notion of security
- Habits, inertia
- Missing security training

Users

- Reluctance to limit themselves
- Ignorance of risks
- Weak awareness

Governance

- Absence of risk management culture in the organization
- Missing interconnection between physical, personnel and information security
- Insufficient records of assets, information classification and categorization of networks and information systems,
- Missing security management in the supply chain

Security operations

- Security centre with 24/7 access or according to business type (also externally)
- Missing vulnerability management
- Missing centralized log collection
- Non-evaluation of logs from operated HW and SW
- Missing access control

Missing areas

- Use of non-updated SW tools
- Weak or no hardening
- Missing backup and recovery plans
- Neglected antivirus tools, tools for e-mail communication protection
- Neglecting the encryption

NATIONAL SECURITY AUTHORITY

NATIONAL
SECURITY
AUTHORITY

" MAYBE WE SHOULD TRY A DIFFERENT SECURITY APPROACH THIS YEAR. "

THANK YOU FOR YOUR ATTENTION

rastislav.janota@nbu.gov.sk

SK NBÚ CERT

NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI