Threat landscape in academic IT

1st Anne Hintzell[1], 2nd Kenneth Kahri [2], 3rd Tero Kärkkäinen[3]

[1]University of Helsinki IT Center, PO Box 28, FI-00014 University of Helsinki, Finland,
anne.hintzell@helsinki.fi
[2]University of Helsinki IT Center, PO Box 28, FI-00014 University of Helsinki, Finland,
kenneth.kahri@helsinki.fi
[3]University of Helsinki IT Center, PO Box 28, FI-00014 University of Helsinki, Finland,
tero.karkkainen@helsinki.fi

Keywords
information security, IT security, threats, cybercrime

1. ABSTRACT

In this paper we introduce you to the University of Helsinki's point of view to general threat landscape in academic IT and many of the ways we have tried to accomplish our goals in mitigating the risk posed by both the external and internal threats based on our experience of which we have drafted a list of agents countering which we consider a priority. On the technical side we describe out monitoring tools and processes. On the non-technical side, the user still remains the crucial factor in causing and preventing IT security incidents. We will brief you in our efforts in educating users in various roles and keeping the security awareness on a good level. The key to successfully design countermeasures for both new and traditional threats is to carry out systematic risk analysis regularly.

2. Introduction to IT Security management at University of Helsinki

Large part of IT environment is centralized to the Center for Information Technology (IT Center). The IT Center is organized as a separate department. It has a Board assigned by the Rector. The Center is divided into IT administration and IT services.

IT management

IT management handles the University IT sector's direction and strategy. It is run by Chief Information Officer Ilkka Siissalo. The unit is in charge of setting the IT architectures and standards, making blanket purchase agreements, managing the centralized information security services of the university and the strategic planning of the information security sector, and monitoring the development of the sector's services, volumes, and expenses.

IT services

IT services is in charge of both the centralized IT services and the IT services produced in the service centers of campus areas. It is run by IT Service Manager Eija Heiskanen. The Service Managers are in charge of their respective services. The service production is divided into four subunits:

Technology Services is responsible for maintaining the server and network infrastructure, production-related maintenance of databases, user administration systems, network services, data traffic, storage space services, technical information security and central management of workstations.

IT Solutions primarily serves the units of the university. Its duties include the support and coordination of IT system projects and acquisitions, IT center project portfolio management and application development, as well as coordination of quality work and development of operations. The subunit is also responsible for the support of teaching and research, video services, and unit communications.

Centralized Support primarily serves user customers. It is in charge of consulting services, software, and workstation services.

Local support provides close-support services at campuses and handles physical maintenance of workstations.

2.1. IT security organization

As per University of Helsinki's IT security policy (https://www.helsinki.fi/en/it/information-security/information-security/information-security-policies-and-terms/university-of-helsinki-information-security-policy), the management and monitoring of information security are incorporated into the University's general management system and are ultimately the rector's responsibility. Each head of department is responsible for the security of the systems it owns as well as for their costs and compliance with rules. The chief information officer is responsible for the main guidelines, strategic guidance and monitoring of information security as well as for the ensuring of sufficient resources for the University's central information security activities.

IT security services are organized within IT management as a team supervised by Information Security Manager Anne Hintzell. Current size of the team is four full-time persons: three specialists and the ISM. The team supports and assists departments in ensuring information security and provides information security training and internal audits. The team also provides incident handling and digital forensics services, develops security related guidelines and monitors state of information security at the University. Some of the technical security related operations such as firewall management and centralized anti-malware software are handled by respective units within the Technology Services.

Internally the team shares assignments in order to ensure everyone has at least sufficient skills in standard operations. This allows all team members to develop expertise in narrower subject matters as routine tasks do not spend all of individual's working time. Skill-wise the team's core competencies are:

- Auditing
- Data protection/privacy
- Digital forensics
- Incident handling
- Intrusion detection
- Risk management
- Vulnerability assessment

3. General threat landscape in academic IT

3.1. Evolution of threat agents

We've come a long way from 1990s and TCB who broke into 130 organizations - including University of Helsinki - just to see if he could do it. He was later caught and convicted and nowadays forges a career as a security consultant. The first half of the 2000s was still predominantly time of amateurs vying for bragging rights. It was to come to an end soon enough: The Blaster worm in August 2003 was the last non-monetized mass infection we've observed in our networks. All epidemics and most cases of external origin, starting with IRCBots in 2004, have since been driven by clear motivation to gain illicit benefit from victims' systems.

All across the spectrum adversaries' methods and tools have improved tremendously during the last 10 years. The progress has been especially fast during last couple years when intelligence agencies' tools and exploits have leaked. The current trend seems to lead towards greater equalization of tools, tactics and procedures between different agents. This both makes the lower level agents more dangerous and leads to even more severe difficulties in distinguishing agents from one another. Further propelling the advance is constantly growing turnover for cyber-crime. In global scale yearly revenues for cyber-crime groups are easily in the millions of euros, tens of millions for the more successful operators, while the whole sector reaps in billions of euros annually. Inevitably part of this money is spent on research & development of both tools and business models. Cyber-crime as a service and gamification of attacks are phenomena unlikely to go away.

For Higher Education Institutions to keep abreast of these development is problematic to say the least. Whereas the criminals can derive direct benefit from improving their processes, the defenders must incur directly increased costs and can demonstrate only indirect benefits in the form of reduced losses, notoriously hard to quantify.

3.2. Common threat agents relevant to academic IT

Although there are relatively many identified classes of threat agents not all of them are equally relevant in academic setting. In most cases Higher Education Institutions as organizations are not interesting enough to be primary targets to those agents dealing in high-value fraud or IP theft. Majority of the users are students who in general do not have much to steal besides identity.

As knowledge producers Higher Education Institutions hold copious amounts of information so ransomware could be conceived as an elevated threat but apparently it seems to target other sectors more often. As scientific research is by definition reproducible ransoming research data may not be as devastating from victims' point of view nor as lucrative from criminals' point of view. Perhaps following from this unlike many other organizations, University of Helsinki not seeing major problems with malware and essentially zero problems with ransomware. Hacktivism-related incidents are a rarity too. Presumably this is partly because University of Helsinki as an organization is politically and ideologically quite neutral, partly because many hacktivists are students themselves.

In the following chapters we will introduce the threat agents we consider to pose the highest risk factor to our IT environment. The list compiled here is based on actual incidents and to lesser degree estimates on how University of Helsinki's threat landscape could develop in the short term. One must keep in mind that these categories are not clear-cut nor universal. There are always exceptional operatives who buck the trend.

Amateurs

Amateurs are relatively indiscreet and indiscriminate with their targets. Threat-wise they do not pose serious problems to defend against and if they are successful cause mostly nuisance and mild embarrassment to administrators. Usually judicious use of firewalls and professional systems maintenance are sufficient to keep these players at bay.

Typical examples of agents in the group

- Script kiddies
- Defacers

Typical incidents

- SSH brute-force attempts
- Automated use of ready-made tools and exploits

Lower-tier cybercriminals

The bulk of all cyberattacks originates from this category of agents. Loosely bound together by motive, financial gain one way or another, they utilize nearly all attack types and vectors commonly observed. Effective defenses must be built in depth on top each other and should include both extensive technical and administrative controls. Especially important part is end-user training as many of the methods rely on social and human aspects.

Typical examples of agents in the group

- Spammers
- Phishers
- Botmasters

Typical incidents

- Drive-by downloads
- Phishing
- Emailed malware
- Automated scanning and exploitation of newly discovered vulnerabilities

Professional cyber criminals

High-level cybercriminals don't necessarily view Higher Education Institutions as primary targets. This doesn't mean Higher Education Institutions are not targeted at all. As we are soft targets with high amounts of technical resources we are useful conduits to route attacks to other organizations and in some cases researchers have financially interesting knowledge such as patentable inventions or unreleased research that may be sought after by some unscrupulous agents.

To mount effective defenses a Higher Education Institution would need highly skilled and well-financed security team and professionally designed security controls implemented in comprehensive way along with mature security awareness program along with strong support from the top management.

Examples of agents in the group

- Organized crime
- Professional hacker teams

Typical incidents

- Sophisticated phishing
- CEO scams
- Targeted hacking attacks with prior research

Insiders

In any organization the insiders are poised to inflict the worst damages. Barring a few large scale breaches it has been the insider who caused or threatened to cause the largest single damages. Human nature being what it is, it doesn't take much of a minor disagreement to escalate into open conflict unless it is dealt with immediately. What makes the situations very delicate is the fact that most often the people involved are authorized to handle the data and IT necessarily doesn't have any indication of problems before it is too late.

Defending against insider threats is a complex subject which leans heavily on administrative and management controls and leadership capabilities of those in charge. Enlisting your organization's legal department's is a very valuable tool too to enforce the administrative directives. Technical controls do not have an effect on the root causes but can reduce and in some cases prevent damage after the situation has escalated.

Examples of agents in the group

- Careless or negligent users
- Disgruntled staff or students
- Terminated employees
- Dishonest or unethical academicians

Typical incidents

- Loss of data
- Unintended publication of information
- Blackmail
- Sabotage
- Misuse of employers' assets
- Fraud

4. Risk-based IT security development

IT security development tends to rely heavily on the demand for compliance. Standards and frameworks provide an overall checklist to what tasks IT security development should consist of. At the University of Helsinki the IT security development follows the relevant legal obligations and regulations, the recommendations from VAHTI - the Government Information Security Management Board as well as good information security practices. These provide a comprehensive manuscript for IT security: f. ex. a list of things to demand from the IT providers or a checklist for IT system development. Frameworks and standards can be of best use in the centralized IT to provide a certain level of security to administrative systems. While focusing on requirements and compliance, the frameworks fail to initiate discussion on threats and risks. This discussion with data and system owners, responsible leaders as well as system administrators is a crucial part of IT security planning.

IT solutions for science and research need to be planned with the primary goal to support the key activities. Information security has to be built based on a risk evaluation rather than filling out a compliance form. In the academic world one solution rarely fits all.

5. Building awareness programs and measuring user awareness

5.1. Awareness training for staff

Regrettably awareness training for staff has been and will still for some time be a weakness for UH. There has not been a comprehensive training program nor requisite training materials. We are moving to remedy the situation but comprehensive coverage will take time. As a first phase action we have created a concise on-line course for staff and are rolling it out to IT and administrative services staff as we speak.

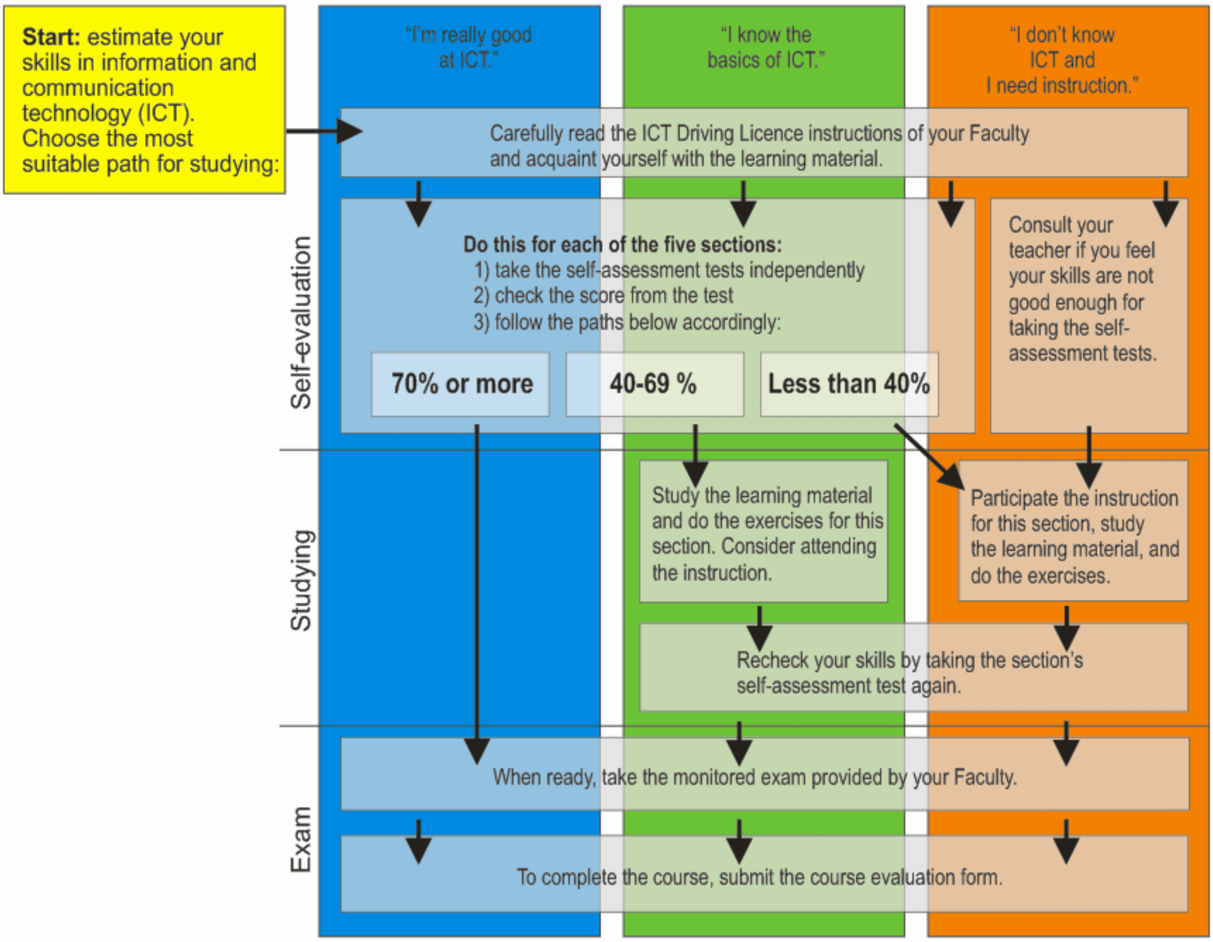
A distinct problem with all training is getting the audience's attention. Without putting requisite attention into understanding what the training is about the audience forgets more easily. And since an average person forgets as fast and much they do, longer-term retention rates are not very good unless engaging methods are found.

The difficulty is especially pronounced when the subjects are something people perceive as tedious, boring and irrelevant, like administrative, legal, contractual, ethical and security matters. The obvious solution is of course making the training mandatory. However especially in academic organizations such action may be viewed with disdain and many could consider it a breach of academic freedom. There is also a question of who should be exempt from the training. Again there is an obvious answer: since the matter is serious enough to warrant making it mandatory there should be literally no exemptions. Which naturally means everyone including the Rector should attend and depending on Higher Education Institution's organization the Board or equivalent external steering group too. It is sufficient to say this would be a serious test to the highest management's support.

5.2. Awareness training for students

All students must successfully demonstrate possessing necessary ICT skills by passing ICT driving license -course (https://www.helsinki.fi/en/ict-driving-licence). The course includes a chapter regarding information security and privacy protection. Security chapter introduces the basic security and privacy principles and motivates the student by walking them through basic steps to protect oneself. The course itself in worth 3 ECTS credits and has been a part of degree requirements in all faculties since 2005.

The course itself is designed to be one of the first courses a student attends to and relies heavily on self-evaluation. Students start off by acquainting themselves with the learning goals and then proceed evaluate their skills by taking five short self-assessment tests. If they score high enough they can proceed directly to exam otherwise they're steered to self-study materials and if needed to faculty-run instruction lessons.



Start: estimate your skills in information and communication technology (ICT). Choose the most suitable path for studying:
"I'm really good at ICT."
"I know the basics of ICT."
"I don't know ICT and I need instruction."
Carefully read the ICT Driving Licence instructions of your Faculty and acquaint yourself with the learning material.
Self-evaluation
Do this for each of the five sections:
1) take the self-assessment tests independently
2) check the score from the test
3) follow the paths below accordingly:
Consult your teacher if you feel your skills are not good enough for taking the self-assessment tests.
70% or more
40-69 %
Less than 40%
Studying
Study the learning material and do the exercises for this section. Consider attending the instruction.
Participate the instruction for this section, study the learning material, and do the exercises.
Recheck your skills by taking the section's self-assessment test again.
Exam
When ready, take the monitored exam provided by your Faculty.
To complete the course, submit the course evaluation form.

Image 1: Flow chart of the ICT Driving license course

Based on relative scarcity of security related incidents regarding students we estimate the ICT driving license largely accomplishes it's security goals by ensuring every student has at least the basic understanding of common threats and risks.

5.3. Quest for the effective awareness training

Over the years we have tried multiple methods and techniques to raise security awareness. The following chapters will introduce many of them along with our observations of their usefulness. It is hard to quantify their real effect as we have not conducted any proper research in to the matter nor have we suitable performance indicators to gauge possible changes.

Poster campaign supported by themed web pages

Of the tools we've utilized old-fashioned poster campaign has garnered the most positive feedback. Using catchy posters to direct viewers to instructional web pages about one bi-weekly changing subject seemed to resonate with both students and staff at the time. The style was deliberately chosen to be light, colorful, tongue-in-cheek even, to pique by-passers' interest. The posters were placed at or very near to buildings' main entrances to ensure maximum visibility and posters' rotation was carefully orchestrated to maintain uniformity across campuses.

Though the poster campaigns are fondly remembered the cost of running them is rather high. One needs resources that may not be easily or cheaply available such as graphical designers and copywriters and large part of the work cannot be cleanly reused elsewhere later on. Things have also moved on, nowadays posters by themselves would not be able to elicit much attention without support from corresponding social media component.

Quiz and small prizes

In one awareness campaign we ran an on-line quiz and awarded a small prize - a key lanyard - to all who completed the quiz with full score. The campaign ran for 4 months during which the quiz was taken 1834 times. It was possible to take the quiz as anonymous user, in which case the possibility of getting a prize was forfeit, or log in with university account and take a chance to win. There were 676 unique logged in users of which 436 managed to land a full score but apparently the prize wasn't worth getting as 334 of them never fetched their lanyard. Anonymous users took the quiz 732 times. Average score was 8,51 for anonymous and 8,97 for logged in users (out of 10).

Although we did not try to count unique anonymous users it was obvious that the quiz failed to reach nearly all students and staff as combined total number of the two groups was approximately 48000 at the time. Proportioning the coverage versus the required effort and monetary cost to create the quiz with prizes showed clearly that cost-benefit ratio was rather bad.

Tailor-made security training

As a part of information security team's service portfolio we create and arrange tailor-made trainings by request. Our experiences have been mostly but not universally good.

Some years ago after receiving numerous requests from individuals to run trainings on specific subjects we arranged multiple different open sessions on several campuses. Attendance was very low, below the number of requestors. It didn't seem to have an effect whether we organized the training in connection with a wider awareness campaign or as standalone events.

On-demand training requested by departments or units has proven to be far more pleasant and more useful. These events are prepared together with the requesting unit and often approach the chosen subject from their point of view. Usually the event is comprised of a lecture and a Q&A session. For more technical subjects we have most often opted for a combination of lecture and hands-on practise.

Mandatory training lectures for IT staff

University of Helsinki had to lay off staff in 2016. In these circumstances the IT management felt it was useful to remind IT personnel about administrators' responsibility and due care and diligence issues. In order to accomplish the goal the IT security team ran a series of lectures and all IT Center's employees were ordered to attend one. The 2-hour lecture consisted of walking through relevant policies, rules, regulations and laws regarding data protection, classification, proper handling and possible sanctions of improper actions.

As expected, mandatory presence was frowned upon and some employees appeared to try avoiding the lecture. The circumstances undoubtedly had a negative effect on would-be attendee's perception too. Feedback regarding the lecture's content was mostly positive though. As a part on compliance requirements set by the GDPR we're retaining the lecture and require all new IT staff to attend it. It remains to be seen whether we will require all staff to attend the lecture on yearly basis in the future.

Adopting an enterprise-like approach and requiring all University staff to attend mandatory yearly training session on subjects such as ethics, security and privacy would no doubt be a sure way to demonstrate legal compliance and improve awareness but such top-down order does not necessarily sit well with academic staff.

On-line course

Traditional instruction materials are one-way and do not have elements that would engage the reader in a meaningful way. More interactive on-line courses have proven to be effective and provide better learning results so both in attempt to heighten awareness and better respond to GDPR's requirements the newest addition to our toolkit is an on-line course.

Technically the course is deployed on Moodle and contains four main chapters with an exam at the end of each chapter.

- Information security at the University
  - Contains subchapters "Why is information security important to everyone? " and "How to work securely?"
- Data processing and classification
  - Contains subchapters "Processing different types of data" and "Storing data and cloud services"

- Office and other locations
    - Contains subchapters "Security and information security at the workplace", "Information security of remote and mobile work", "Email security" and "Email encryption"
- Information security incidents

The IT security team collects statistics on course completion and provides corresponding supervisors information whether their subordinates have completed the course. Although the exams are graded they are provided for attendees' benefit and not used to rank people; answering all exam questions is sufficient to pass the course. This is done on purpose as the of the course's functions is to be an objective tool for self-evaluation.

At the time of writing this the course and it's English translation have been out for so little time that data regarding it's efficacy is not yet available. Pilot groups' feedback has been positive. In general the respondents have felt the contents is understandable and useful to them though some exam questions have been flagged as overly ambiguous. The first production deployment will be University Services on second quarter of 2017. This unit consists of approximately 1000 administrative staff. This should provide us with large enough sample to gauge usefulness and effect.

On the national level a number of Finnish universities have created together a generic multi-module on-line course for staff covering the most important subjects in academic IT security. University of Helsinki was not able to participate earlier but is currently considering joining in the effort.

Specific warnings during elevated threat levels or ongoing attacks

During out of the ordinary circumstances we issue targeted warnings about specific threats to groups or individuals we have determined to under elevated level of threat. Usually these warnings consist of an email sent to the targets detailing the threat and the actions they should take to mitigate it. If the target groups are large we issue a generic notification to whole university stating that we are sending out warnings to specific people and they should take it seriously. Examples of such circumstances are notable data breaches outside the University, detected malware infections often targeting certain types of devices and software vulnerabilities affecting IT services not maintained by the IT center.

Direct messaging does get the information to the recipient but it still does not guarantee it is understood nor acted upon. One notable problem with this kind of communication is the tendency of people to try and set the scary issue aside pretending it doesn't exist or trying to deny the need to do anything to protect themselves. One would be well-advised to use the expertise of professional communications staff while preparing the messages and notices sent to the recipients to verify intelligibility in adverse conditions.

5.4. Further training methods under consideration

Continually improving IT staff's security skills is vital as the adversaries' improve theirs. While advising IT administrators we've noticed their understanding of offensive hacking techniques is not always deep enough for them to consider systems' security in a comprehensive and holistic way. As hands-on exercises and gamification are effective ways to motivate people, we are considering setting up an infrastructure to host capture-the-flag -style hacking competitions. This would enable us to train IT administrators to better assess and defend their systems against malicious hacking.

The basic idea would be to let voluntary participants form an number of small teams who would then compete against each other by scoring points from different tasks ranging from quiz questions to hacking attacks in simulated environment. The platform would allow honing technical hands-on skills, teaching administrative aspects such as reporting, incident handling process and provide bridge from technical guidelines to reality.

5.5. Measuring security awareness

Currently we haven't got a good method to measure users' security awareness. Some conjecture can be gleaned from incident statistics and types of tickets opened with IT security team but precise this information is not. In the future the on-line course will provide statistical data on coverage and relative skill level. Likewise the students' ICT driving license provides its own statistics but both courses lack indicators on how well people are able to apply the things they learned.

Many IT security consultancies provide different services to measure the organizations security posture and awareness in real world. One feature we have considered is measuring our user's resiliency against phishing by authorizing and contracting a consultancy to conduct life-like phishing attacks against our users. By targeting statistically significant sample we should be able to gain far more precise data on how and what kind of phishing fools the users. This would allow us to identify what specific areas we would need to improve in awareness training.

6. Monitoring and auditing IT environment

6.1. Environment sections

The current IT environment of the university of Helsinki is large and heterogenous. It consists of different tiered systems. They come with varying threats, and managing it requires constant monitoring and auditing to be able to assess the current security level and to react to newly found weaknesses.

Network infrastructure

Providing the physical layer of access to data. This means firewalls, routers, network switches, wireless access points. Our network teams handle network planning, management and monitoring mainly focusing on the usage levels and providing sufficient bandwidth to users. Any anomalies in usage levels can be monitored and detected.

- Netflow data is gathered for statistical analysis and for forensic use
- Network firewalls gather statistics on possible DDOS attacks, intrusion attempts
- Bandwidth usage is monitored

Server instances

These vary from physical rack servers to virtual servers, most managed by our server management teams, not forgetting cloud-based services (SaaS), Both Linux and Windows servers are numerous and tend to be very highly standardized. Some specialized server instances are jointly managed by our teams (The base OS) and external consultants (Applications) while some are completely external (Cloud-based computing).

Server teams rely on automated checks and keep the server and virtualization infrastructure up to date. Some security-related logs are centrally collected. Server managers have access to and are encouraged to use our vulnerability scanner to check the systems they are responsible for.

Workstations

The vast majority of workstations 0are running standardized Microsoft Windows. There are also a lot of OS X computers and Linux computing, predominantly in our hard sciences units. All employee computers are centrally managed, and come with our own security customizations.

Local firewalls and antiviral software forward alerts to a central management system. Workstation operating system and application installations and updates are centrally managed and monitored. User data is mostly stored on proper storage infrastructure.

BYOD

There are workstations that are owned and maintained by their owners. We have no control on these devices, and we provide our users with suggestions and guidelines on how they can be used. Because of their nature and inherent risks, BYOD devices are only allowed on the wi-fi networks or ethernet networks with similar access restrictions.

Other devices

IoT in building automation, classroom AV equipment etc. A real can of worms. This is a problematic area, as these devices are often purchased by the building administration office and are can be either very old or sometimes not designed with any network security implications in mind. Network scanning can also disturb the proper working of these devices. They are isolated from production networks as much as possible.

6.2. IT Security team's tools

The IT security team employs automated network vulnerability scanning and compliancy checks:

- Discovery scanning for new devices that have appeared on the local network, and those that are exposed to the internet
- Scanning for open ports and services
- Identifying the services and software versions in use
- Probing for known vulnerabilities
- Alerts and statistics

These checks are automated and recurring. This gives us historical perspective on the vulnerabilities a system may have.

Intrusion Detection System

A smaller subset of servers and workstation networks that deal with more sensitive data are subject to more scrutiny.

All IP packets are inspected, and possible intrusion attempts cause alerts. Suspicious traffic is stored and can be examined later if needed for forensic study.

Honeypots

As network monitoring is typically router-based, computers on the same LAN subnet can communicate between each other without being detected. Only the local firewalls on servers and workstations report such traffic.

To gather intelligence and situation awareness in our visitor and BYOD networks, we're employing honeypots. These are Linux servers with software that answer on all ports and even try to mimic real-life server software. All traffic is logged and reported, and presented on a dashboard that provides a quick view of the situation and how the possible threat levels are changing. We typically can see misconfigured devices and port scanning attempts in these networks.

Penetration testing

New services are penetration tested before they are taken into production use. Depending on the data sensitivity level and total threat assessment, testing can be done in-house or using external consulting firms.

Work to be done:

In order to maintain compliance with GDPR, some form of SIEM system should be implemented to maintain a complete overview and to allow for quicker reaction time to events.

7. AUTHORS' BIOGRAPHIES

Anne Hintzell is the Information security manager of University of Helsinki. Anne holds an M.Sc degree in computer science and a CISSP certification (ISC^2). Anne has worked in the IT field since 2004, focusing mainly on IT security and enterprise architecture.

Kenneth Kahri is an IT security specialist at the University of Helsinki. He has worked with academic IT since 2002 and in IT security since 2004. As a member of University's CSIRT team he has been considerably involved with incident handling and digital forensics.

Tero Kärkkäinen is an IT security specialist at the University of Helsinki. He has a background in server and network management, having run the UH video management systems and network operations for 16 years. Tero is now using his experience to the benefit of the CSIRT team, handling technical aspects of threat assessment and mitigation.