Computer Security at CERN

DR. STEFAN LÜDERS

Stefan Lüders, PhD, graduated from the Swiss Federal Institute of Technology in Zurich and joined CERN in 2002. Since 2009, he has headed the CERN Computer Security Incident Response Team as CERN's computer security officer, coordinating CERN's office computing security, computer center security, GRID computing security, and control system security while taking into account CERN's academic environment and its operational needs. Dr. Lüders has spoken on computer security and control system cybersecurity topics to international bodies, governments, and companies on many different occasions, and has published several articles. Stefan.Lueders@cern.ch

Computer security is often seen as a technological problem: encryption, network anomaly detection, central (mobile) device management, firewalls, cloud-based SIEMs—each deemed to be the panacea. However, technical solutions fall short when dealing with a free and open academic environment like that of CERN, the European Organization for Nuclear Research. The CERN Computer Security Team faces the daily challenge of appropriately balancing CERN's operational and research needs with a reasonable level of computer security. At CERN, computer security is largely seen as a sociological problem. The first line of defense sits in front of the screen. Raising computer security awareness among CERN's 15,000 users is imperative to avert computer security incidents. Technological means, while still important, come second.

Introduction

CERN, the European Organization for Nuclear Research (or, according to its original French acronym, le Conseil Européen pour la Recherche Nucléaire; http://cern.ch), is one of the world's largest and most respected centers for scientific research. Its business is fundamental physics, finding out what the universe is made of and how it works.

CERN hosts a large complex of so-called particle accelerators and colliders, all providing insight into the subatomic structure of those particles. Accelerators boost beams of particles to high energies before they are made to collide with each other or with stationary targets. Detectors observe and record the results of these collisions. These records allow physicists to study the properties of the particles and learn about the laws of nature. Very often, a single experiment involves a collaboration of several hundred if not thousands of people from all over the world. Currently, several dozen different experiments are in operation at CERN, detecting collisions from half a dozen different particle accelerators, including the world's most powerful one, the Large Hadron Collider (LHC).

Besides seeking and finding answers to questions about the universe, CERN is advancing the frontiers of technology, bringing nations together through science, and training the scientists of tomorrow. CERN's 2250 staff members welcome about 15,000 guest physicists and visiting collaborators (so-called "users") annually. Because the particle experiments are international, CERN's users come from hundreds of universities, organizations, and laboratories from all over the world. In fact, only a few countries have never sent citizens to CERN. And the turnover is high: Students join CERN during their summer vacation to follow additional lectures, contribute to dedicated projects, and initiate their careers; BSc, MSc, and PhD students come to CERN for a few months (or years!) to attend seminars, receive training, and conduct, prepare, and finally write their theses; post-doc physicists join ongoing collaborations to advance their careers and satisfy their interests; professors regularly visit CERN to stay in touch with their CERN-based teams and their colleagues, for workshops, or to attend or give lectures; engineers and technicians arrive to install their technical equipment in CERN-based detectors or accelerators; young people do internships at CERN, in administration or one of the technical sectors. In parallel, many of those users connect remotely to

CERN's computing facilities to conduct analyses, simulations, or solve engineering problems. Alternatively, they can use the Worldwide LHC Computing Grid (WLCG), a network of major computer centers around the globe with CERN being its headnode (the so-called "Tier-0"), to conduct large-scale analysis of physics data—we are talking about several petabytes of accumulated data sets produced by individual experiments.

Thus, CERN not only presents a working environment to users, it also provides private accommodations and hostels on CERN premises, restaurants, and recreational facilities. CERN hosts several dozen different clubs for after-work hours (e.g., microelectronics club, car club, running club, yoga club, music club). In fact, professional and private life at CERN is pretty much entangled, giving users the necessary environment and freedom to pursue their research.

Academic Freedom versus Security

With such a vast academic user community and so many different cultures, nationalities, interests, and aims represented, standardization is unrealistic. From an IT perspective, users can bring their own laptops with their favorite operating systems in any flavor or language (the "BYOD" trend has existed at CERN for a while); developers can program in their favorite programming language; users can run any software tool or program and deploy whatever technological means they deem necessary to reach their goals. In that respect, CERN can be seen as an ISP and computing service provider for its users. Furthermore, users are accustomed to exchanging ideas, sharing information, and publishing results freely. Web sites can be created at the convenience of the users. In short, CERN hosts a vast academic environment that relies on freedom of choice and freedom of communication. It is not without reason that the World Wide Web was proposed 25 years ago by a CERN employee, Tim Berners-Lee.

CERN's Computer Security Team (https://security.web.cern.ch/security/home/en/index.shtml) has to find the right balance between CERN's academic environment, the safe operation of its accelerators and experiments, and its computer security. While this academic freedom makes for a very dynamic and innovative environment, with new systems and services being deployed all the time, it also increases security risks to our computing. CERN's Computer Security Team is mandated to minimize both the likelihood and impact of security events; to prevent and protect against digital attacks; and to maintain premium detection and response capabilities.

Although the environment is "free" at large, CERN users cannot act as if they are in a void. Use of CERN's computing facilities is governed by a set of lightweight policies (https://security.web.cern.ch/security/rules/en/index.shtml) that set rigid limits on what is allowed and what is not. Although "users can bring their own laptops," for example, they are required to guarantee the laptops' security and apply prompt patching; whereas "Web sites can be created at the convenience of the users," the contents must not be offensive or illegal; although "users can run any software tool or program," they are still bound to obey copyrights and license conditions. In addition, any usage must neither be detrimental to the workings of the organization nor significantly affect computing resources (e.g., computing power, disk space, network bandwidth). For example, generating crypto-currencies on CERN-owned computing clusters or running Nmap scans without explicit authorization by the CERN Computer Security Team is prohibited. The CERN computing rules even provide the framework for the private use of CERN's computing facilities: While private and personal usage is generally tolerated, illegal, inappropriate, or offensive activities are banned, and violations lead to administrative measures.

However, the most important feature of CERN's security paradigm is delegation. While the CERN computer security officer is mandated by CERN's director general to coordinate all aspects of computer security at CERN through prevention, protection, detection, and response, he is not the person ultimately responsible for all computer security at CERN given the heterogeneous environment, and the academic freedom that comes with it, and given the consequently limited leverage of control. Instead, at CERN, staff and users individually assume primary responsible for the security and protection of their computers, the operating systems they run, the applications they install, the software they program, the data they own, and the Web sites they maintain. Service and system managers are responsible for ensuring that their services and systems run securely, are maintained, and follow good security practices. Project managers are responsible for the security of their projects, and the line management for that of their constituency.

Basically, at CERN, "computer security" is dealt with in the same way as safety. Safety cannot easily be ignored: If there is a puddle of water on the floor, it is my personal responsibility to prevent people from slipping on it, and I cannot just relegate this to the building's safety officer. It's the same for security. Still, this does not mean that users are singly responsible for their own security. The CERN Computer Security Team (nominally four staff and a few students) provides assistance, consulting, and help in order to enable CERN's staff and users to fully, effectively, and efficiently assume that responsibility. CERN's IT department provides the necessary common tools and general services for the Computer Security Team and, more importantly, for CERN's user community: Instead of managing and patching their own PCs, users can obtain a centrally managed PC and antivirus software which is kept up-to-date by the IT department. The IT department provides Web servers, content management systems, databases, file storage systems, and engineering applications that are properly managed, adequately secured, and maintained over the long run. In short, users can delegate their responsibility for security to the IT department and avoid the burden of managing "security" themselves. Instead, they can focus on their core work. Still, it is up to the users and each experiment to opt in. They are encouraged to do so, and usually do.

Security Training

With such a heterogeneous community, user awareness, education, and training are paramount. Users are often the weakest point in the security chain, are not necessarily aware of computer security issues, and do not always feel concerned. It is hard for them to really assume the responsibility imposed on them by the CERN Computing Rules. Thus, a trigger is needed to raise their computer security awareness or—even better—to educate them such that they understand security risks. Ideally, this is supposed to introduce a cultural change in the same way that young children can be taught to swim or to look left and right before crossing a street. Once certain practices become engrained, safety on the road or in the pool is automatically and subconsciously guaranteed. For "security," we need the same automatism, (e.g., when receiving a "phishing" email or when prompted to install a new program).

Therefore, all new CERN users receive an introductory course on computer security matters when they arrive at CERN. This course is paralleled by an online course followed by a 10-question multiple-choice quiz to be successfully passed in order to obtain a computer account giving access to CERN's computing facilities. This course and quiz must be renewed every three years and is aligned with similar courses on safety. In addition, various awareness campaigns are given periodically to all CERN units to reiterate the main security messages: "Protect your computers," "Be careful with email and the Web," "Protect your passwords," "Protect your files and data," "Respect copyrights," and "Follow the CERN Computing Rules." These six primary messages basically apply to everyone, everywhere, not only those at CERN, and the course encourages people to apply security principles at CERN as well as at home. A series of videos, posters, and handouts complement these campaigns and provide additional information. Overall, the Computer Security Team collaborates with the CERN Human Resources department to better integrate security knowledge, awareness, and behaviors into existing processes and situations.

The power of these awareness campaigns can be measured via the number of passwords lost to "phishing": In 2008, 40 of about 1500 CERN recipients of a crude phishing mail divulged their password to the attackers. A subsequent analysis has shown that neither age, gender, attitude toward technology, salary, nor "intelligence" determines the likelihood of succumbing to phishing. Instead, what counts (for the attacker at least) is the moment. Many affected recipients that we interviewed stated that they were busy with something, saw the mail from "Webmail IT service," and answered it just to get rid of it. Only later did it occur to them that the "Webmail IT service" might not have been necessarily CERN's. Today, after three years of awareness campaigns, CERN loses only about two to three accounts to such emails per month. Given the more than 20,000 active users and high turnover, this is deemed acceptably low.

Still, these awareness campaigns are just seeds. Once people understand that "security" is part of the overall IT phase-space containing "functionality," "usability," "availability," and "maintainability," they naturally ask for more. This is the moment when users ask the CERN Computer Security Team to consult with them before starting new IT projects, for penetration testing, and for assessing the security footprint of new systems and the auditing of existing deployments. It is also the moment for dedicated training: For software developers and system experts, the Computer Security Team, in collaboration with the CERN's Technical Training team, provides optional in-depth training sessions on developing secure software, secure Web application development, as well as dedicated sessions on secure coding in C/C++, Java, Perl, Python, and for Web applications. In the past, these courses have been quite successful, with attendees from all different areas within CERN.

In addition, a series of static code analyzers were made available to all developers in order to further improve their code: Coverity and flawfinder for C/C++, FindBugs and CodePro's Analytics for Java, RATS for Perl/Python/PHP, pychecker for Python, and Pixy for Perl. The configuration of those tools is simple, and, admittedly, these code analyzers will never find all flaws. However, even in their basic configuration they help developers to easily detect at least some potential security weaknesses (both functional bugs and security vulnerabilities). Once developers see these benefits, they are open to additional steps towards a "security" mind-set: enabling and checking on compiler warnings and error messages; employing more sophisticated code analyzers; doing full code reviews; embracing a full-blown secure software development life cycle; and, finally, employing sophisticated tools for software management and integration with nightly builds, regression testing, and permanent scanning for weaknesses, sub-optimal configurations, and flaws. Once developers are at this level, security worries are diminished.

Vulnerability Scanning

Preventive training is good, but verification is also necessary. Currently, CERN has registered on its public-IP networks about 180,000 devices (PCs, laptops, smartphones, tablets, etc.) by their MAC address, and it controls access through RADIUS/MAC-address-based authentication. About 80,000 have been seen active use during the past months. While MAC-address spoofing rarely happens, this is usually quickly detected and followed up as a violation of the CERN Computing Rules. CERN's main computer centers alone host about 10,000 servers, 100,000 cores, and 75,000 hard disks, which currently store more than 100 PB of data (http://information-technology.Web.cern.ch/about/computer-centre). The CERN identity management system currently lists more than 36,000 CERN personal accounts plus about 8500 accounts for special purposes (e.g., database accounts, generic accounts for running automatic services). Its central Web service holds more than 12,000 Web sites (e.g., https://security.web.cern.ch/security/home/en/index.shtml) on more than 3 million Web pages using Sharepoint, Drupal, J2EE, CGI/ Python/Perl scripts, or plain HTML. A few hundred more Web servers are managed by individuals (users) for dedicated purposes that cannot be easily served by the central Web services (e.g., Web sites requiring proprietary software or database integration).

The Computer Security Team, therefore, actively and permanently scans major computing resources for vulnerabilities. All Web sites hosted at CERN are regularly scanned for vulnerabilities using Skipfish (a tool published by Google) as well as with Wapiti and w3af. Additional tools produce an inventory of all Web sites, Web applications, and Web technologies used on individual hosts, and compare this with a list of vulnerable or outdated versions. Similarly, the level of protections of all devices connected to CERN networks is regularly assessed using Nmap, which subsequently gives another valuable inventory of currently running services and their versions. A dedicated custom-scanning suite dubbed Prodder probes deeper into particular security issues (e.g., writable folders on Windows PCs, outdated myPHPadmin frameworks). CERN's centrally managed file systems and software repositories are regularly scanned for exposed (i.e., public) credentials like private SSH keys as well as for inconsistencies in their access configuration: A “private” folder should never permit access to everyone holding a CERN computing account. Finally, devices that require access from the Internet, like Web servers, have to undergo dedicated scans using Nessus and Skipfish. Usually, the results indicate the quality of the server setup and its security. Only servers that successfully passed the scans will be granted that access through CERN's outer perimeter firewall (the firewall hardware is maintained by the CERN Networking Group, but its configuration is maintained by the Computer Security Team).

Essential for such permanent scanning is a comprehensive and all-encompassing asset inventory: Devices (and their respective firewall openings), accounts, and Web sites must have a registered owner taking over the responsibility entrusted to him or her. Lots of effort has been made to ensure that this inventory is permanently up-to-date and accurate. Other computing services are automatically assigned to an organic unit within the CERN hierarchy, which, thus, provides the necessary contact points in case of security issues. A recent project has been launched to further improve on this and have a life cycle for any computing resource used at CERN. Although declaring new resources (accounts, Web sites, devices, etc.) is always based on the incentive of the requestor, the resource life cycle will ensure that there is also an incentive once the registered owner leaves CERN. The resources are passed on to a new owner, assigned to the leaving person's supervisor, or destroyed.

Thanks to this proper asset inventory, all potential vulnerabilities can be communicated directly to the corresponding owner of the affected account, file space, Web site, or device, and must be mitigated. The Computer Security Team's Web-based event management system provides all necessary tips and tricks to allow users to mitigate these findings themselves. Alternatively, the IT department and the Computer Security Team once more provide assistance and help. Only in rare cases does the Computer Security Team need to take a harsher stance and block the Internet access of a certain Web site or disconnect a certain device from the network (not having permanent access to Facebook has been proven to be a good incentive to act quickly). On average, only three to six such blockings are executed per month. In all cases, the tight interaction with the users also opens up an opportunity to advertise the aforementioned training sessions.

For high-profile Web sites and vital computing services, the Computer Security Team offers in-depth reviews and security assessments. Dedicated so-called “Security Baselines” provide users with a short list of good practices for securing their computing servers, Web servers, or file servers.

Incident Response

Despite all of these preventive measures, incidents inevitably do happen. The Computer Security Team has deployed a series of sophisticated, intrusion detection means-monitoring activities on centralized computing facilities and on CERN networks in general.

These means include the centralized monitoring of the antivirus software installed on all centrally managed Windows PCs by colleagues from the Windows Support Group, the detection of malicious domains and IPs in DNS requests and in all network traffic, deep-packet inspection using “Snort,” the statistical analysis of network flows (“netflows”) indicating abnormal behavior, and the analysis of computer logs. All sensors run on standard Computer Center hardware managed by the IT department and configured through IT's “Agile Infrastructure” (i.e., Puppet, OpenStack, Git, etc.). The data analyses are fully automated, and any owner of an affected device is automatically notified of a malicious security event. Once more, the team's

Web-based event management system provides all necessary tips and tricks to allow users to mitigate these findings themselves. The mail system automatically suspends any mail activity if more than 3000 mails have been sent during one day. Alternatively, the user is assisted by the Computer Security Team's first line of support in solving the identified issues. More severe incidents are handled by the Computer Security Team's CSIRT (Computer Security Incident Response Team).

Summary

CERN's user community is vast and is used to the spirit of academic freedom and free communication. It is difficult (impossible?) to centralize or standardize the necessary computing environment without spoiling this freedom, and so a heterogeneous environment is prevailing at CERN. Given this special challenge, the Computer Security Team had to tightly involve CERN's users: At CERN, users are primarily responsible for the security and protection of their assets. The Computer Security Team provides assistance and help, with a primary focus on education and culture change. Once "security" is part of the average user's mind-set, the overall level of security should further increase. Until then, sophisticated detection and protection means have spared CERN from too many too-visible security incidents. The Computer Security Team is working hard to maintain this status quo.

usenix

THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

Buy the Box Set!

Whether you had to miss a conference or just didn’t make it to all of the sessions, here’s your chance to watch (and re-watch) the videos from your favorite USENIX events. Purchase the “Box Set,” a USB drive containing the high-resolution videos from the technical sessions. This is perfect for folks on the go or those without consistent Internet access.

Box Sets are available for:

- **URES ’14:** 2014 USENIX Release Engineering Summit
- **USENIX ATC ’14:** 2014 USENIX Annual Technical Conference
- **UCMS ’14:** 2014 USENIX Configuration Mangement Summit
- **HotStorage ’14:** 6th USENIX Workshop on Hot Topics in Storage and File Systems
- **HotCloud ’14:** 6th USENIX Workshop on Hot Topics in Cloud Computing
- **NSDI ’14:** 11th USENIX Symposium on Networked Systems Design and Implementation
- **FAST ’14:** 12th USENIX Conference on File and Storage Technologies
- **LISA ’13:** 27th Large Installation System Administration Conference
- **USENIX Security ’13:** 22nd USENIX Security Symposium
- **HealthTech ’13:** 2013 USENIX Workshop on Health Information Technologies
- **WOOT ’13:** 7th USENIX Workshop on Offensive Technologies
- **UCMS ’13:** 2013 USENIX Configuration Mangement Summit
- **HotStorage ’13:** 5th USENIX Workshop on Hot Topics in Storage and File Systems
- **HotCloud ’13:** 5th USENIX Workshop on Hot Topics in Cloud Computing
- **WiAC ’13:** 2013 USENIX Women in Advanced Computing Summit
- **NSDI ’13:** 10th USENIX Symposium on Networked Systems Design and Implementation
- **FAST ’13:** 11th USENIX Conference on File and Storage Technologies
- **LISA ’12:** 26th Large Installation System Administration Conference

Learn more at: www.usenix.org/boxsets