IT-Security @ Freie Universität Berlin

By Christoph Wall, Director of Administrative IT, Freie Universität Berlin (Germany)

When computers first came into operation to work specific tasks designed to crack Enigma's code in Bletchley Park, nobody would have considered anyone of the handful of specialists able to program the machine a potential risk, e.g. as somebody who would willingly employ his programming skills to design code that would harm or lead the machine to malfunction. The machine was invaluable in helping to decode German military communication, and therefore harm through one of the dedicated specialists working on the program was never considered.

If Bletchley's machines had remained one of a kind, or computers had not spread more than anticipated in the infamous quote *"I think there is a world market for about five computers"* attributed to IBM's CEO John Watson in 1943, the problem of IT-Security would have remained a problem similar to that of keeping an expensive piece of equipment safely stored away from harm like theft or physical vandalism.

However, computers spread beyond the wildest beliefs of anyone who had witnessed their humble beginnings in parents' living rooms or garages. They took over critical tasks like computing the statics of bridges and the deployment of nuclear weapons. With this prominence, computers started to be seen as a potential risk, in case of failure. Consequently, in the early eighties the first ideas arose that speculated about malicious programs infecting computers like a virus.

It did not take long for these speculations to become reality. In 1986, the first computer virus was detected on a mainframe at Freie Universität Berlin. In the same year two programmers from Pakistan wrote the first virus for PCs. This PC virus spread widely in 1988 and was named "Brain" because it's main function was to rename specific folders on infected machines to "brain". "Brain" spread through infested floppy disks and it was purportedly meant to protect the intellectual property rights of a widely copied program the designers of "Brain" had written.

After the internet had brought real momentum to the number of computers, connecting them worldwide it opened the way to large scale activities in the field of malware proliferation. The first virus, that spread big time and purportedly lead to damages of 10 Billon US Dollars, was a simple love letter that contained in its code a program that could stop computer operations altogether. “I love you” therefore marked a turning point in the utopian romantic beliefs about the internet being the way to finally bring peace to the world by giving democratic access to information for everybody regardless of status, personal wealth, nationality etc.

Nowadays, every comprehensive IT-Strategy comprises IT-Security as an essential element. The Digital Agenda for Europe as given out by the European Union names “Trust and Security” as their third pillar. The German government founded the “Federal Office for Information Security” in 1991. It provides one of the most comprehensive catalogues of measures to secure IT-systems. The IT-Strategy of the Freie Universität Berlin lists IT-Security as one of its six strategic goals.

Prominent as we have now found IT-Security to be, it becomes necessary to look into what we can actually expect of it and what it can help us to achieve. The German “Office for IT-Security” defines the values IT-Security is supposed to protect. These are displayed below:

Confidentiality: information that is confidential must be protected against unauthorized disclosure

Availability: services, IT system functions, data and information must be available to users as required

Integrity: data must be complete and unaltered

The “IT-Grundschutz” (IT-Basic-Protection) guideline, from which these values are taken, then goes on to explain what the central elements of an IT-Security Management System are:

Governance

Risk assessment or analysis: A risk analysis provides information on the probability of the occurrence of a damaging event and its negative consequences.
Security policy: In a security policy, the security objectives and general security safeguards are formulated in the sense of the *official regulations of a company* or a public authority. Detailed security safeguards are contained in a more comprehensive security concept.

Technical

Authentication:
When a person logs into a system, the system runs a check in an authentication process to verify the identity of the person. The term is also used when the identity of IT components or applications is tested.

Authorization:
Authorization is the process of checking whether a person, an IT component or an application is authorized to perform a specific action.

Data protection:
Data protection refers to the protection of personal data against misuse by third parties.

Data backup:
Data backup involves making copies of existing data to prevent its loss.

In the field of Governance, the Freie Universität Berlin has given itself a comprehensive set of guidelines, directives and bye laws that regulate many aspects of the use of IT for all members. The four dimensions to be covered by those regulations are

1. the definition of the elements and bodies of the organization and their responsibility with regards to IT
2. the regulations regarding data privacy for systems using personal data
3. the aspects of IT useage that impact the workplaces and job-descriptions of the employees
4. the practical matters that have to be regulated to make organized use of IT-resources feasible

Beyond the governance aspects which regulate the use of IT so that the data stays confidential, available and intact, technical provisions have to be taken to make sure this gets realized. The following paragraphs will introduce important components that the SAP system supplies to make the IT-environment secure. The aspects to be addressed will specify:

- Identity Management

- Authentication

- Role based Authorization

- Layers of security for Web-Portal-Access to SAP backend

- Security Optimization Self-Service (SOS Report)

- Action log for intrusion detection

- Backup and Restore Support

Identity Management at the Freie Universität Berlin is realized through a system of interconnected components out of SAP and non-SAP environments. Our main goal in Identity Management is to connect the involved components in a way that removes the need for manual input after a person is employed at the Freie Universität Berlin and has been entered into the HR system. The same holds true for students who are automatically given their digital identities after enrolment.

To achieve this, a person's data needed for the creation of his or her digital identity is communicated from HR to the SAP IdM Identity Management System. There it is put into the identity store and the information is passed on to the FU Directory System FUDIS where an account as imprint of the digital identity is issued and further communication data, like a telephone account for our VoIP system is procured. All this data is returned to IdM and finally ends up in infotype 105 in the HR system. Individuals who are teachers are provided with the role "teacher" by IdM and a user with the corresponding rights is created in the SLcM Campus Management system. The same mechanism is used to provide students with their user ID's and rights in the SAP environment. Upon termination of contract or withdrawal the digital identities are automatically deactivated and all access rights are withdrawn.

When a person is equipped with an account, user and rights that person can logon to the SAP Portal that provides access to an ever widening amount of **el**ectronic **s**ervices of the **a**dministration (elsa). The logon process is a Shibboleth based federated Single Sign On that gives out a token which admits use of all "elsa" systems, including a Web-Dispatcher. This opens access to the portal, which works in a certificate-based trusted relationship with the actual backend system on which the process requested by a user runs. Within the portal itself the Freie Universität, Berlin plans to implement a two factor authentication based on SAML2 that enables each portal application to specify the required security level. Therefore, critical services like the changing of address data or unlocking of passwords can be secured more strongly than, for example, access to statistical data and other reporting functionality.

To monitor whether the security measures taken in the diverse and complex landscape of the SAP system are satisfactory, SAP provides the so called SOS (security optimization service) Report. This report can be run on the different SAP systems in use to check if there are still any risks to be found. The report itself comes as an extensive word document and states its purpose in the preface as:

The ***SAP Security Optimization Service*** is a comprehensive support service that identifies security risks for your SAP system and helps you to determine the appropriate measures to protect it from these risks.
The security checks of SAP Security Optimization are performed for the following security aspects:

- **Availability:** ensuring that a system is operational and functional at any given moment

- **Integrity:** ensuring that data is valid and cannot be compromised

- **Authenticity:** ensuring that users are the persons they claim to be

- **Confidentiality:** ensuring that information is not accessed by unauthorized persons

- **Compliance:** ensuring that the system security set-up is in accordance with established guidelines

Since the SOS report is generic and can be run in large or small scale environments, the risks pointed out have to be interpreted in relation to their impact on the particular SAP environment. This can be commented on in the document so that an IT-security officer can check at a glance whether there are still topics open that would need further attention. The Freie Universität Berlin runs the SOS report twice a year and discusses the most important findings and adjustments to the system in the yearly IT-Security review.

Even if all imaginable measures concerning IT-Security have been taken, it is still necessary to keep a watchful eye on IT-systems. Even though unauthorized intrusion to the system is blocked in many ways there will always be malicious activities by individuals with criminal intent towards the organization or to gain unearned personal advantages. Therefore, it is necessary to monitor the critical activities going on within the system or at its gates.

For this purpose SAP provides the Security Audit Log. This report can be configured to what the administrator of a system wants to monitor. At the Freie Universität Berlin we check failed logon attempts in all systems, downloads out of the system, start of batch jobs and other events that might be potentially dangerous. The amount of monitored event types should be specified bearing in mind that there must be enough time to analyse the output of the report. It may be wise to monitor less so you don’t overlook the rare critical incident in a huge mass of day to day trivia.

Finally, it must be considered that not just malicious intrusion endangers the security of the data in an IT-System. There is always a chance that a program runs into a critical state because a rare condition occurs against which it was not properly tested or a hardware problem corrupts the data. In this case, it is essential for business continuity that all data prior to and as close as possible to the occurrence of the corrupting event can be reconstructed. To take care of this the SAP system is equipped with a comprehensive backup environment that at the Freie Universität Berlin is configured in a way to write logs saved away on an hourly basis. A daily differential backup is written every night and once a week a full backup is made.

To conclude, it can be said that keeping data safe is a challenging job. The environment required for the safe running of an SAP system is very complex. Even though a lot of automation and system support is supplied within the SAP administrative environment, there is still quite a bit of time consuming work for the admins left to do. On top of all this: work for the safekeeping of data usually remains unseen. Security when it works properly is invisible.

However, in the end everybody is better off invisibly safe than visibly sorry.

Christoph Wall

Mr. Christoph Wall received his PHD in Philosophy from the Technische Universität Berlin in 1989. He started his professional career the same year as a teacher for subjects pertaining to philosophy and informatics at the department of philosophy, theory and history of science at Technische Universität Berlin. From 1992 until 1994, he was project manager for the implementation of hospital information systems. From 1994, with SAP’s entrance into the health care market, responsibilities shifted to the initiation and management of a team of SAP health care consultants and the solution design for hospitals and hospital groups in Europe and Canada. In 2009, Mr. Wall entered the world of higher education as head of administrative IT at Freie Universität Berlin and serves in this role to date.