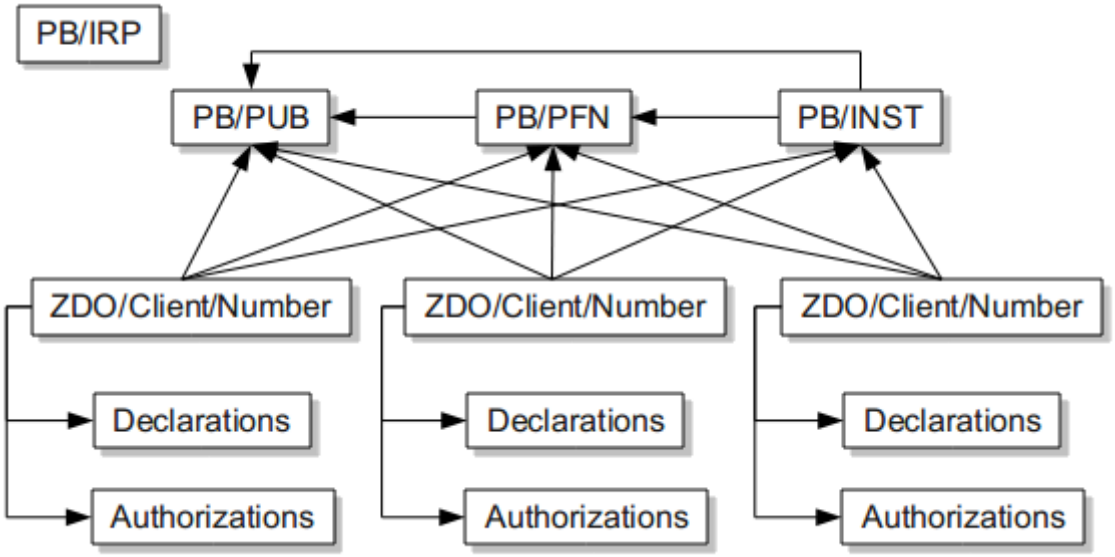
Vertabelo Security Whitepaper

Overview

At Vertabelo and e-point SA (Vertabelo mother company which provide hosting services), we take security very seriously. The security of our applications and hosting environments has held center stage since the day we opened for business. During our formative years, security consciousness was drummed into everyone who worked here – not only administrators and developers, but also producers, managers, office clerks and even janitors.

Since 2004, we have in place a formal security policy to cover every system developed and/or hosted by Vertabelo/e-point SA. We clearly defined some of the rules that had been implicit, organized our documentation, and made sure that our security policy complied with the requirements laid down by the General Inspector for the Protection of Personal Data so that our Customers could rest assured that whatever personal data they made available for processing would be protected. We also provide assistance in registering data files.



Dependencies between documents related to systems security

Arrows indicate documents referred by more detailed documents. As part of the task described here, we have developed the following documents:

- PB/PUB — "Security policy, public part".
- PB/PFN — "Security policy, confidential part".
- PB/INST — "Instructions for managing an information system that processes personal data".
- PB/IRP — "Procedures for detected security breaches".
- ZDO/Customer/Number — description of personal data.
- Statements — statements of employees with access to the personal data file.
- Authorizations — authorizations for employees with access to the personal data file.

It quickly became clear that such an abundance of hardcopy documents was going to be difficult to manage. We therefore created a dedicated IT system to support the management of personal data protection and any associated documents the system generated.

The PB/IRP document shown above was added in 2010, when the increasingly critical role of the systems we were supporting and the growing risk of network incidents forced us to define a procedure and establish mutually acceptable means of customer contact and steps to follow in case of an incident.

We do not believe in "security through obscurity", but obviously we cannot reveal everything we do to ensure the systems we manage are secure. The information presented here is therefore general.

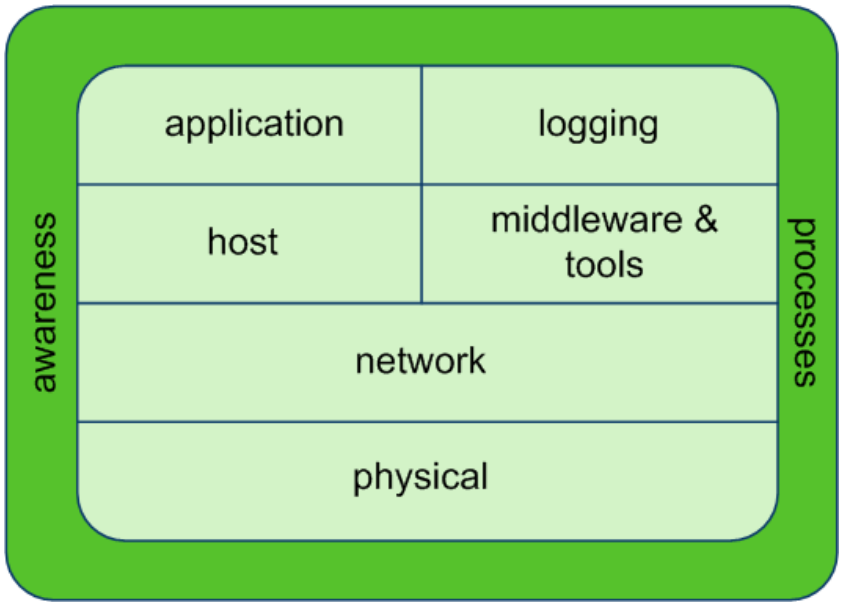
Holistic Approach

Security is a fairly thankless task, as it involves saddling people with procedures and restrictions they dislike. Moreover, there is no direct return on investing in security – just a lack of problems that is difficult to quantify. We will have to put the more appealing issue of systems deployment to one side for a moment and think about possible contingencies, how to prevent them, and at what cost. Numerous publications, conferences, and experts have been devoted to security. Nor is there any shortage of security measures. Some are good (simple and effective), some not so good (complex and ineffective).

At Vertabelo/e-point SA, we have adopted three security principles:

- Security must be approached holistically — the hosting environment is only as secure as its weakest link.
- Components that have to be implemented in every hosting environment managed by Vertabelo/e-point SA – with no ifs or buts – need to be defined.
- The cost of a security measure must be proportional to the value of the data it protects.

Security is a very broad topic that covers everything from the physical security of buildings, networks, servers, middleware and applications through to the education of Vertabelo/e-point SA staff and system users. Consider the diagram below:



Awareness and Processes

Our holistic approach to security begins with a security conscious work culture that builds security awareness among all Vertabelo/e-point SA staff, including Board Members, who voice their support for the procedures we deploy and approve the necessary expenditure.

Security is not a state, but a never ending process. Although the concept of continuous improvement is a process, it is not enough. We have appointed two Security Specialists to make increasing security a more conscious process:

- An administrator who focuses on all the hosting environment components (networking, firewalls, etc.), and
- A programmer who focuses on sharing knowledge related to developing secure systems.

Both areas are vitally important. However, the information available here and abroad indicates that attackers can most easily breach security through the following attack vectors:

- Web application errors, e.g. XSS, CSRF
- Human errors, e.g. weak passwords or phishing vulnerabilities.

So, apart from hosting, it is very important to educate programmers, web developers and end users on using proven technologies that seldom have serious vulnerabilities, especially to remote exploits. Our Security Specialists are responsible for internal education. Our staff also attend external training sessions, including hands-on workshops.

Recruitment is another process we use to bolster security. That's right. We believe that our people (including our administrators) are our most valuable asset. Our recruiting procedures are lengthy and thorough. We interview many applicants before making our final selection. Our team members are all ethical professionals, and we have a very high staff retention rate. This is the perfect, and purposefully chosen, component of our security measures against “insider threats”.

We should also mention another process that keeps our system security efficient, effective and up-to-date — we analyze log and monitoring reports, and keep track of new technologies as they become available.

Physical Layer

The term “physical layer”, as used here, has nothing to do with the ISO/OSI model, but refers to the physical components that need to be protected against physical threats, viz. buildings (e.g. the hosting center and company premises), equipment rooms, and hardware. Security measures are required to protect these components from theft, willful damage, and natural disasters (fire, flood etc.).

We leave the security of our hosting center to ATM, a telecommunications company with which we have been collaborating since 2004. ATM server facilities are modern buildings with security zones, electronic locks with access control, access lists, surveillance cameras and guards, while the utilities necessary for reliable operation, such as energy, air conditioning and network connections, are delivered with appropriate redundancy.

Network

The network layer should comprise traditional IT security measures. This layer involves the following security components:

- Firewalls.
- Separation of physical and virtual networks.
- Communication encryption: SSL, SSH, IPSec.

Middleware

Security at the middleware level is based on several choices:

- *Careful selection of Open Source software*. We choose widely used, actively maintained software (some Open Source projects are naturally abandoned) with frequent security patches available and even, in some cases, a well-defined release cycle process. Good examples of reputable and actively developed software are Apache, PostgreSQL, and the Linux Debian and OpenBSD operating systems.
- *Focus on selected commercial products*. We have strong skills with certain commercial products. You cannot be good at everything, so we have focused on IBM for AIX, DB2, WebSphere and TSM, and Oracle solutions for databases and application servers.
- *Using Java Virtual Machine (JVM)* as our application runtime platform. JVM introduces an additional degree of separation between the operating system and the application. JVM is yet another security layer that has to be breached before an attacker can exploit a potential bug in the system software. This might seem impossible today, but the situation could change tomorrow. There has never been a remote code execution or privilege escalation attack on a Java Virtual Machine running as a server (not to be confused with client-side Java, where the picture is no longer so clear).

Finally, we should not overlook more obvious measures, such as frequent updates, running software in user mode where possible, configuration control, and changing default options and passwords.

Operating System

A lot can be done at the operating system level, both in technological and psychological terms. There even exists a separate knowledge domain called OS hardening. There are system distributions that focus mostly on security, and existing software packages that improve resource access management. The problem is that greater security adversely affects usability and even can even diminish the capabilities of the system. Moreover, it increases the cost of system management considerably.

We have evaluated the risks and determined how to protect our operating systems. Our basic security measures are:

- Restricting the services available to those necessary
- Event logging
- Not providing full access to operating systems to anyone outside Vertabelo/e-point SA.

Logging

Event logging is worth highlighting in a separate section, because we believe it is a crucial aspect of protecting the system and ensuring its long-term stability. Logs can be analyzed automatically or semi-automatically against anomalies, value fluctuations, frequency of exceptions and errors, intrusion attempts, etc. In the case of a successful security breach, these logs help us conduct investigations, trace attack sources and vectors, and provide evidence to law enforcement agencies.

System logs need to be looked at comprehensively. Log sources do not just include the operating system, but also applications. The firewall and application server can be valuable sources of information as well.

Application

By analyzing current threats generated by the Internet, we can clearly see that the main point of security breaches is the application. At Vertabelo/e-point SA, we spend a lot of our time minimizing the dangers that arise from badly written applications. This section highlights this attack vector as the one that requires most attention, and discusses the security measures used to achieve this. To summarize:

- Appointment of an application Security Specialist.
- Our own platform with embedded mechanisms to help build secure applications.
- Staff training.

The Open Web Application Security Project (OWASP) has played a crucial role in organizing knowledge about secure Web applications. We test our applications against OWASP recommendations. Some are mandatory, but others are not applicable to our applications or have specific functional consequences.

Our applications have been audited for security several times. In fact, we encourage our Customers to do this. Security is a struggle against probability and human weaknesses — we can never rule out the possibility that something has been overlooked. For us, every audit is an opportunity to hone our skills and improve security for all our Customers.