

DRŽÍME TI MÍSTO!

Pracovní příležitosti
pro absolventy vysokých škol

www.hp.cz/4students



*HP Security
Framework
Jakub Andrlé*



Hewlett-Packard

- 11. place in Fortune Magazine chart
- In fiscal year 2007 we achieved \$7bilions growth
- CEO HP - Mark Hurd, company residence - Palo Alto, California, USA
- **HP CZ**
 - On the Czech market from 1967
 - HP CZ established 1993, before HP Československo
 - 900 employees, 3 branches
 - Important projects: Letiště Praha, VZP, T-Mobile, Vodafone, ČNB – Help desk, Kapsch Telematic Services, DHL

HP for students and graduates

- **Graduate Development Program**

- possibility to grow up from graduate to young professional during 12 months program with individual development plan. Determined for graduates or students in last year study of technical, IT or economy area

- **Internship program**

- Determined for students in third and higher years of study that have interest to develop their work experience during study. Possibility to work in consulting & integration, outsourcing, software development, logistics, purchasing, marketing, finance and business departments

- More information at www.hp.cz/4students

Agenda

- HP Security Framework
 - How HP come to solve information security
- Security Testing
 - What everything could be security testing



HP Security Framework

Key points to note about security are ...



It's not just about technology, but people and process also



It's a journey, not a destination



Security is built in, not bolted on



It's about balance between the threat costs vs. prevention

HP's solution approach

- Addresses IT operational risk in the areas of people, process, systems and the external environment
- Security solutions built to meet three core business objectives in which governance is pervasive throughout
- More than technology - a holistic approach that includes the people and processes



Governance



HP can help establish an effective security governance framework allowing the assessment of risk to all assets and the implementation of appropriate mitigation plans in accordance with standards, laws and business requirements.

Risk assessment services

- In-depth analysis of current security posture
- Comparison of security measures to industry standards
- Recommendations for reducing exposure to currently identified security risks

Security strategy & architecture services

- Set of services to improve business and security control through all components of the governance lifecycle
- Security architecture methodology

Compliance services

- Understanding compliance status, and identifying non-compliance areas
- Resolution of non-compliance through solution design and implementation
- Monitoring and measurement of key control indicators

Training & awareness services

- Ensures that users and practitioners perform at their best, and play their part in safeguarding critical information assets.

Governance - services

- Risk Analysis
- Risk mitigation plans
- Security strategy and policies development
- Assessment of information weaknesses and risks
- Law and regulation compliance
- Security architecture
- Security processes
- Security measurement and monitoring
- Security audits and compliance assessments

Identity Management



HP provides fully automated access and provisioning solutions based on its market leading OpenView software products implemented through a proven services process methodology.

Identity management services

- Identifies and manages every user, application and device to provide flexible authentication, access control and auditing capabilities
- Tools for creating, maintaining and terminating a digital identity designed to cope with dynamic user environments and business change
- Solutions in the areas of identity provisioning, directory integration and access management and federation
- Leverages technologies from the HP OpenView portfolio, as well as selected partner technologies
- Tightly coupled combination of product and services process methodology – implementation in accordance to ITIL

Identity Management - services

- Solutions for identity management and privileges
- Use of strong authentication (chip cards, biometrics etc.)
- AAA (authentication, authorization, audit)
- Single Sign-on
- Complete public-key infrastructures (PKI), including processes and policies
- PKI-based application security

Proactive Security Management



HP provides a coordinated solution involving people, processes, tools and technology, which proactively manages information security threats, vulnerabilities, and incidents in order to minimize their impact on key business processes.

Proactive security management services

- Coordinated strategy of involving people, processes, tools and technology to minimize the impact of security threats
- Vulnerability management, security incident and event management and countermeasure solutions
- Management of all aspects of the threat environment in a fully integrated manner
- Complete solution addressing security needs throughout the security management lifecycle

Security incident & event management services

- Security monitoring and management services that provide ongoing vigilance and maintenance
- Enables organisations to maintain more effective defences and mitigate current and potential threats

Proactive Security Management - services

- Analysis of threats and reactions to threats
- Intrusion detection and reaction
- Incident response
- Detection of weaknesses
- Investigation and forensic services
- Incident and patch management
- Security Monitoring
- Virus and other malware countermeasures

Trusted Infrastructure Management



HP provides trustworthy infrastructures which assure confidentiality, integrity and availability of data and processes by securing resources according to the level of trust required by the business.

Trusted infrastructure services

- Building resilient and reliant security infrastructures through a focus on people and process as well as products
- Security architecture design
- Adaptive Network Architecture (ANA)
- Host, network, end point security and client security
- Centralised network policy management
- Data encryption and secure collaboration solutions
- Application protection
- Infrastructure design review and implementation

Security support services

- Support and maintenance services for a wide range of hardware and software products – including product installation & configuration
- Customised 24x7 remote & onsite support for multi-vendor security hardware and software products to ensure business continuity

Trusted Infrastructure Management - services

- System hardening
- Data encryption
- Trustworthy domains
- Applications security
- Network security policy management
- Perimeter and portal security
- Electronic channels security

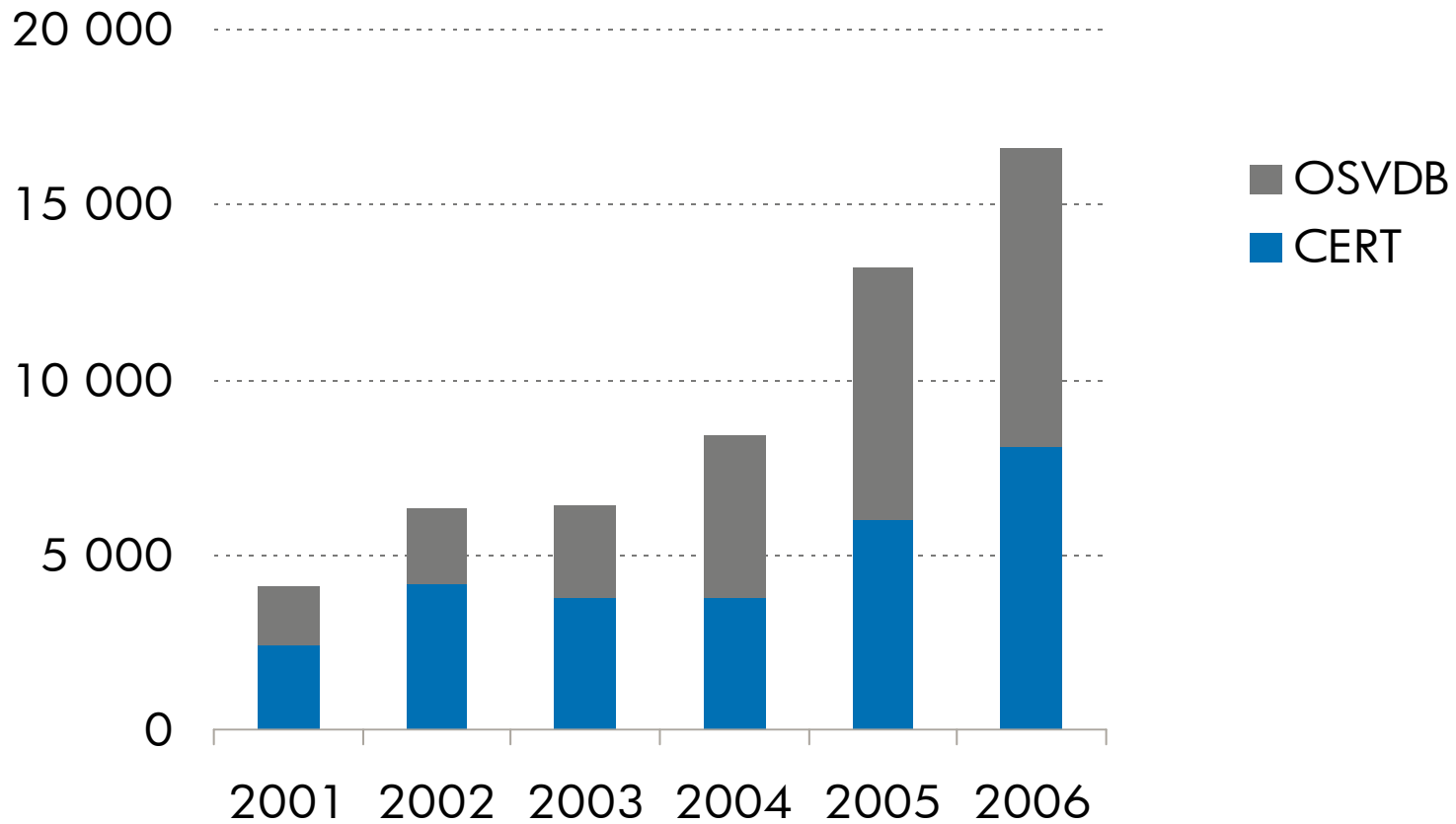
HP Security

- HP Security Services
<http://www.hp.cz/security>
- HP Security handbook
<http://www.hp.com/go/security>



Security Testing

New Vulnerabilities Trend



Source Area: CERT/CC, Open-Source Vulnerability Database

What can we do?

- nothing
- patching
- training
- monitoring
- testing

What is Security Testing

- Security testing is a process/technique how to identify and verify that our defined level of security is correctly implemented and working
- Test results are describing current status in the time of testing

How can we do it?

- Techniques for identification of our current state
 - Evaluation – passive, manual
 - Identification and analysis – active, automatic
 - Vulnerability validation – active, destructive

Evaluation

- Operational documentation
- Systems configuration
- Application source code
- Security device rule sets
- Policies, procedures, processes
- Logged information

Identification and Analysis

- Mapping and monitoring of network
- Services, ports and protocols
- Vulnerabilities
- Applications

Vulnerability validation

- Password breaking
- Remote access testing
- Penetration testing
- Social engineering

Application Security Testing

Why is application security important?

- Application complexity grows
- Number of new application vulnerabilities grows
- More new and less checked technology are used
- Solutions are focused on web applications
- Web applications are the most attacked target

Price for removing security defects

- Costs for removing of security defect in phase of:
 - design very low
 - development low
 - testing middle
 - Implementation/production big
- Result: Security defect must be recognized at beginning of project. With this approach can be the cost for elimination of security defects minimized

Recommendations

- Focus on application security
- Do security testing at the beginning and in all phases of application development lifecycle
- Find assistance and testing simplification in security testing tools
- Guide for tool selection:
 - Who will use it
 - How it will be used (service, tool, combination)
 - How it will be integrated into current development tools
 - Automation, usage of signatures, reporting possibilities

How security testing can help

- Prevention and mitigation of losses due to growing complexity and quantity of vulnerabilities, threats and incidents
- Minimizing of impact to business, good name and customer satisfaction due to verification of our defined security requirements
- Verification and documentation of law and regulation compliance
- Draw the attention to defects in actual protection
- Detection of broken security measures



Questions?

**Thank you for your
attention**

Web: www.hp.cz/4students

Email: kariera.cz@hp.com

