Rev 0.6 Thursday, November 08, 2007
Rev 1.0 Monday, November 26, 2007

A data security threat assessment case study

Abstract

A formal data security threat assessment was performed for a publicly traded advanced technology manufacturing company during the months of October-November 2007. The objectives for the study were to evaluate the internal and external threats that impact the company's digital assets. Using the Business threat modeling (BTM) methodology, a risk model was constructed and populated with threat scenarios. Data was collected using structured interviews and network surveillance performed using a Fidelis XPS appliance. Assets were valuated by the CFO and IT security operations and technologies were valuated by the CIO. The output of the study was a cost-effective, prioritized program of data security controls – this program was presented and approved by the management board of the company. The detailed threat model was provided to the client and is currently used on an ongoing basis to perform what-if analysis and track the data security implementation.

Conclusions

1. The bulk of the security budget is currently spent on sustaining network perimeter security and system availability. Not surprisingly, these countermeasures are not particularly effective in mitigating insider threats such as lost or stolen hardware and information leakage, which now dominate the company's risk profile.

2. **In corporate IT Security operations**: The two major data security systems that were purchased in 2007, Imperva and Fidelis XPS have not yet been fully implemented and do not provide the expected benefit. To be specific, Imperva needs to be able to produce real-time alerts on violations based on logical combinations of OS user, DB application and DB user. Fidelis needs to be deployed in the subsidiaries. Monitoring from both systems needs to become a daily operational tool for the security officer.

3. **In the Asia Pacific region**: Loss of notebooks to the tune of 2-3 / quarter is a major vulnerability although content abuse of the corporate network is assessed as negligible due to cultural factors.

4. **In general**: Publicly facing FTP servers must be monitored carefully for violations of the company acceptable usage policy. In the course of the risk assessment, we discovered strategic plans and proprietary source codes that were stored on publicly accessible FTP servers.

Action plan

1. The objectives/key results of the security officer should be based on the optimized risk mitigation plan as described in the **Table 3** below. The work plan of the security officer should be executed according to the sequence of steps in the optimized risk mitigation plan.

2. The threat model should be updated once a quarter in order to track and ensure countermeasure effectiveness.

Top current risk threats

Threat	Value at risk
T034 Internal, employee notebooks may be stolen or lost	12,000,000
T011 Internal, employees may leak sensitive information on Web	7,500,000
T036 External, competitors may use social engineering to obtain data	6,000,000
T022 External, competitors may use reverse engineering to copy products	6,000,000
T030 Internal, employees with privileges may access or compromise Oracle Applications	4,000,000

Summary of assets at risk

System financial value		System Risk status	
Total value of assets	145,486,667	Maximal Value at risk	40.6%
Already invested in mitigation	253,800	Current risk level	35%
Plan 2008 countermeasures	408,200	Minimum risk level	5.9%

Table 1

Assets at Risk – Detailed List

Asset	Description	Yearly Weighted Value
Company reputation	If confidential or proprietary company data is breached, company and its executives' reputation is tarnished, value will be damaged	66,666,667
Company reputation for accurate and on time financial reporting	Company reputation for accurate and on time financial reporting, valuated at company valuation, possibly outstanding stock value + potential third-party claims, 25% of total reputation	50,000,000
The confidentiality and integrity of customer contracts	If contracts are breached or manipulated, financial damage may be caused to the business units that base their transactions on the contract The value of the asset is the maximal annual damage that can be caused by losing business due to disclosure or manipulation of a single contract, calculated as 50% of the value of largest contract that was signed in 2006 = 10% of 1/2 yearly sales of company,	12,500,000
Proprietary product designs, source code for machine software	Proprietary product design and implemented source code - if leaked or stolen may affect ability of company to compete, amortize over a 24 month design cycle. Implications are: 1. Lose dev costs 2. Lose future revenue. Will double the product life, if design goes to competitor who develops a superior machine - lose all development costs - 10M, if same then 5M because revenue will be less -	5,000,000
The ability of the executive and board to maintain confidentiality of M&A plans	The ability of the executive and board to maintain confidentiality of M&A plans is a major factor in gaining (or losing) this reputation. 1. Price will go up - 2. Deal will come apart (future value). The company spends 50-100M to purchase companies each year - 10% of this budget is at risk.	5,000,000
Ability to manage employees and run the company	Ability to manage employees and run the company, would be meaningful impact if a senior manager were impacted, calculated on basis of 1% of revenue	4,000,000
Reliability, integrity and availability of financial reporting data provided by the ERP system	Availability of ERP system for ongoing operations (for example - Sun announcement to vendors and customers after implementation of Oracle Applications). Reliability (for example case of company XXXX), DEPENDS on timing - within 24 hours, marginal damage. Each add'l 24 hours - 1M.day	1,000,000
RFP/RFI pricing and terms	Pricing and terms of the company's response to competitive requests for proposal or information - if disclosed may hurt the company's ability to compete	1,000,000
Employee productivity	If malicious code infects workstations, productivity will be damaged, calculated at 80k/year/250 work days/year x 1.0 work day x /1000 employees maximal damage	320,000
	Total	145,486,667

Table 2

Optimized risk mitigation plan 2008

Starting risk before implementation of planned countermeasures: 35%

Step	Countermeasure	CM Cost	Step Cost	Plan Cost	Residual Risk
1.00	**Monitor unusual file transfers –** Use Fidelis XPS to detect and prevent transfer of sensitive digital assets on public-facing FTP servers	4,000	4,000	4,000	32.90%
2.00	**Training, security awareness for employees and contractors** Prepare training material with HR and deploy in company using a method of "Train the trainers" where work-groups have responsibility for executing the training	18,000	18,000	22,000	
	Monitor acceptable usage violations Use Fidelis XPS to detect abuse of IT resources according to the company's acceptable usage procedure – for example usage of the network by employees for non-work related tasks, consumption of large amounts of bandwidth, surfing to pornographic Web sites that may contain spy-ware/mal-ware.	4,000	22,000	26,000	
	Alert on Web postings of digital assets Use Fidelis XPS to detect transfer of sensitive digital assets on forums and blogs	4,000	26,000	30,000	
	Establish and enforce acceptable usage for insider disclosures Write and approve a 2-3-page procedure for acceptable usage of IT resources by employees. Procedure will be implemented by managers with their direct reports and at the time of new hire orientation.	2,000	28,000	32,000	28.80%
3.00	**Login accounts should be given the minimal rights that are necessary for their functionality** Ensure that employees and onsite contractors do not have wide-ranging rights to access systems and assets outside their scope of work and need to know	20,000	20,000	52,000	25.00%
4.00	**Whole disk data encryption for notebooks** Deploy disk encryption in order to mitigate risk of leakage of sensitive digital assets in the event that a notebook is lost or stolen	90,000	90,000	142,000	
	Removable device control Deploy centrally controlled removable device control in order to mitigate the vulnerability of data theft associated with USB and mobile devices	43,200	133,200	185,200	17%
5.00	**Imperva DB firewall, monitor unauthorized usage of production Oracle** Alert on unauthorized combinations of network user, application and database password	4,000	4,000	189,200	
	Implement Identity mgmt system Support access rights enforcement with centrally controlled identity management system.	60,000	64,000	249,200	
	Training, workplace awareness Proactive training to mitigate risk of sexual harassment	75,000	139,000	324,200	
	Perform software security assessment of publicly facing applications Determine root cause of software vulnerabilities (bugs) that enable attackers to exploit applications and access or modify sensitive digital assets	50,000	189,000	374,200	7.70%
6.00	**Detect unauthorized workstations that bypass proxy servers** Use Fidelis XPS in order to detect users that bypass the ISA server	4,000	4,000	378,200	6.70%
7.00	**Implement new source control system & methodology** Source control system in engineering	30,000	30,000	408,200	5.90%

Table 3 – IT Security operations and acquisitions in Euro not including capital depreciation