Chapter 4.17 Experiences from Using the CORAS Methodology to Analyze a Web Application

Folker den Braber Norway

Arne Bjørn Mildal NetCom, Norway

Jone Nes NetCom, Norway

Ketil Stølen SINTEF, Norway

Fredrik Vraalsen SINTEF, Norway

ABSTRACT

During a field trial performed at the Norwegian telecom company NetCom from May 2003 to July 2003, a methodology for model-based risk analysis was assessed. The chosen methodology was the CORAS methodology (CORAS, 2000), which has been developed in a European research project carried out by 11 European companies and research institutes partly funded by the European Union. The risk analysis and assessment were carried out by the Norwegian research institute SINTEF in cooperation with NetCom. NetCom (www.netcom.no) is one of the main mobile phone network providers in Norway. Their 'MinSide' application offers their customers access to their personal account information via the Internet, enabling them to view and change the properties of their mobile phone subscription. 'MinSide' deals with a lot of sensitive customer information that needs to be secure, while at the same time being easily available to the customer in order for the service to remain usable and competitive. The goal of the analysis was to identify risks in relation to the use of the 'MinSide' application and, where possible, suggest treatments for these risks. This

Table 1. NetCom's Key Figures

	2002	2001	2000	1999	1998
Customers					
Number of customers	1,178,466	1,082,850	900,282	745,089	535,892
NetCom's market share (of total	29%	26%	28%	30%	30%
amount of mobile phone					
customers)					
Total share of mobile	86%	81%	75%	62%	48%
subscriptions in Norway					
Finance					
Turnover/Sales (million NOK ¹)	4,591	3,752	2,914	2,494	2,032
(million USD ²)	670	547	425	364	296
Result/Profit (million NOK)	1,101	725	421	331	103
(million USD)	160	106	61	48	15
Calling minutes per customer per					
month					
Subscription	255	227	214	179	-
Prepaid	63	58	64	79	-
Text messages (SMS ³)					
Total amount (in millions)	-	502	310	157	36

was achieved through two model-driven brainstorming sessions based on system documentation in the form of UML sequence diagrams and data flow diagrams.

ORGANIZATIONAL BACKGROUND

NetCom

NetCom is the second largest mobile phone network provider in Norway, providing solutions for mobile communication. NetCom is an innovative company that uses new technology and knowledge to meet its customers' demands and aims to be a leading company in Norway within the market of mobile communication. A main goal for NetCom is that their products shall be competitive on price and quality, while at the same time remaining easy to use and understand for all its customers. With offices in Trondheim, Bergen, Stavanger, Kristiansand and Tønsberg, and its main office located in Oslo, NetCom has 740 employees in Norway.

NetCom is owned by the Swedish-Finnish company TeliaSonera, the leading telecom com-

Sub process	Description
1 Context Identification	Identify the context of the analysis. Describe the system and its
	environment; identify usage scenarios, the assets of the system and its
	security requirements.
2 Risk Identification:	Identify the potential threats to assets, the vulnerabilities of these
	assets and document the unwanted incidents.
3 Risk Analysis:	Evaluate the frequencies and consequences of the unwanted incidents.
4 Risk Evaluation:	Identify the level of risk associated with the unwanted incidents and
	decide whether the level is acceptable. Prioritize the identified risks
	and categorize risks into risk themes.
5 Risk Treatment:	Address the treatment of the identified risks and how to prevent the
	unacceptable risks.

Table 2. CORAS Risk Management Process

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-

global.com/chapter/experiences-using-coras-methodology-analyze/23199

Related Content

A Holistic View on Blockchain and Its Issues

Mohd Azeem Faizi Noor, Saba Khanum, Taushif Anwarand Manzoor Ansari (2023). *Research Anthology on Convergence of Blockchain, Internet of Things, and Security (pp. 1-20).* www.irma-international.org/chapter/a-holistic-view-on-blockchain-and-its-issues/310436

Technical Report White Paper: Risks of Passengers Overloading in Urban Public Transport in Bahir Dar City

Endalsasa Belay Abitew (2020). *International Journal of Risk and Contingency Management (pp. 54-58).* www.irma-international.org/article/technical-report-white-paper/246847

Predictive Analytics and Data Mining: A Framework for Optimizing Decisions with R Tool

Ritu Chauhanand Harleen Kaur (2014). Advances in Secure Computing, Internet Services, and Applications (pp. 73-88).

www.irma-international.org/chapter/predictive-analytics-and-data-mining/99451

Libraries to the Rescue

Michael R. Mabe (2016). *International Journal of Risk and Contingency Management (pp. 62-81).* www.irma-international.org/article/libraries-to-the-rescue/148214

DNSSEC vs. DNSCurve: A Side-by-Side Comparison

Marios Anagnostopoulos, Georgios Kambourakis, Elisavet Konstantinouand Stefanos Gritzalis (2012). Situational Awareness in Computer Network Defense: Principles, Methods and Applications (pp. 201-220). www.irma-international.org/chapter/dnssec-dnscurve-side-side-comparison/62383