predict
prioritise
prevent

TRESPASS

Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security

Deliverable 9.1.2

Dissemination means: logo, website, brochure, templates, press releases

Project:	TRESPASS
Project Number:	ICT-318003
Deliverable:	D9.1.2
Title:	Dissemination means: logo, website, brochure, templates, press releases
Version:	1.0
Confidentiality:	Public
Editor:	Lorena Montoya, UT
Cont. Authors:	F. Brodbeck, P. Hartel, L. Montoya, W. Pieters, C. Probst, F. Reis
Date:	2013-01-31

Part of the Seventh Framework Programme
Funded by the EC-DG CONNECT

Members of the TRESPASS Consortium

1.	University of Twente	UT	The Netherlands
2.	Technical University of Denmark	DTU	Denmark
3.	Cybernetica	CYB	Estonia
4.	GMV Portugal	GMVP	Portugal
5.	GMV Spain	GMVS	Spain
6.	Royal Holloway University of London	RHUL	United Kingdom
7.	itrust Consulting	ITR	Luxembourg
8.	Goethe University Frankfurt	GUF	Germany
9.	IBM Research	IBM	Switzerland
10.	Delft University of Technology	TUD	The Netherlands
11.	Hamburg University of Technology	TUHH	Germany
12.	University of Luxembourg	UL	Luxembourg
13.	Aalborg University	AAU	Denmark
14.	Consult Hyperion	CHYP	United Kingdom
15.	BizzDesign	BD	The Netherlands
16.	Deloitte	DELO	The Netherlands
17.	Lust	LUST	The Netherlands

Document History

Authors		
Partner	Name	Chapters
LUST	F. Brodbeck	1
DTU UT	C. Probst W. Pieters	2
UT LUST	L. Montoya F. Brodbeck	3
LUST	F. Brodbeck	4
UT GMV	P. Hartel F. Reis	5
UT	L. Montoya	6

Quality assurance		
Role	Name	Date
Editor	Frederic Brodbeck	2013-01-31
Reviewer	Miguel Martins and Carlo Harpes	2013-01-14
Reviewer	René Rydhof Hansen	2013-01-14
WP leader	Dieter Sommer	2013-01-31
Coordinator	Pieter Hartel	2013-01-31

Circulation	
Recipient	Date of submission
Project Partners	2013-01-31
European Commission	2013-01-31

Acknowledgement: *The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TRE$_S$PASS). This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.*

Contents

List of Figures

List of Tables

Management Summary

This report contains a collection of dissemination material to be used by partners. This includes logos, the website, the brochure, the powerpoint templates, the deliverable template which is available in LateX and in Word format as well as the text of the press releases. Also included is the bibliographic information about press coverage in printed form and the URLs of the online press coverage. There is no chapter for the deliverable template, but this deliverable has been formatted according to such template.

1 Logos

Figure 1.1: Logo versions

2 Website

The website is up and running since October 11th, 2012. Regarding its design, it is divided into the following pages: home, project partners, news, documents and contact. It is available in the following URL: https://www.trespass-project.eu/

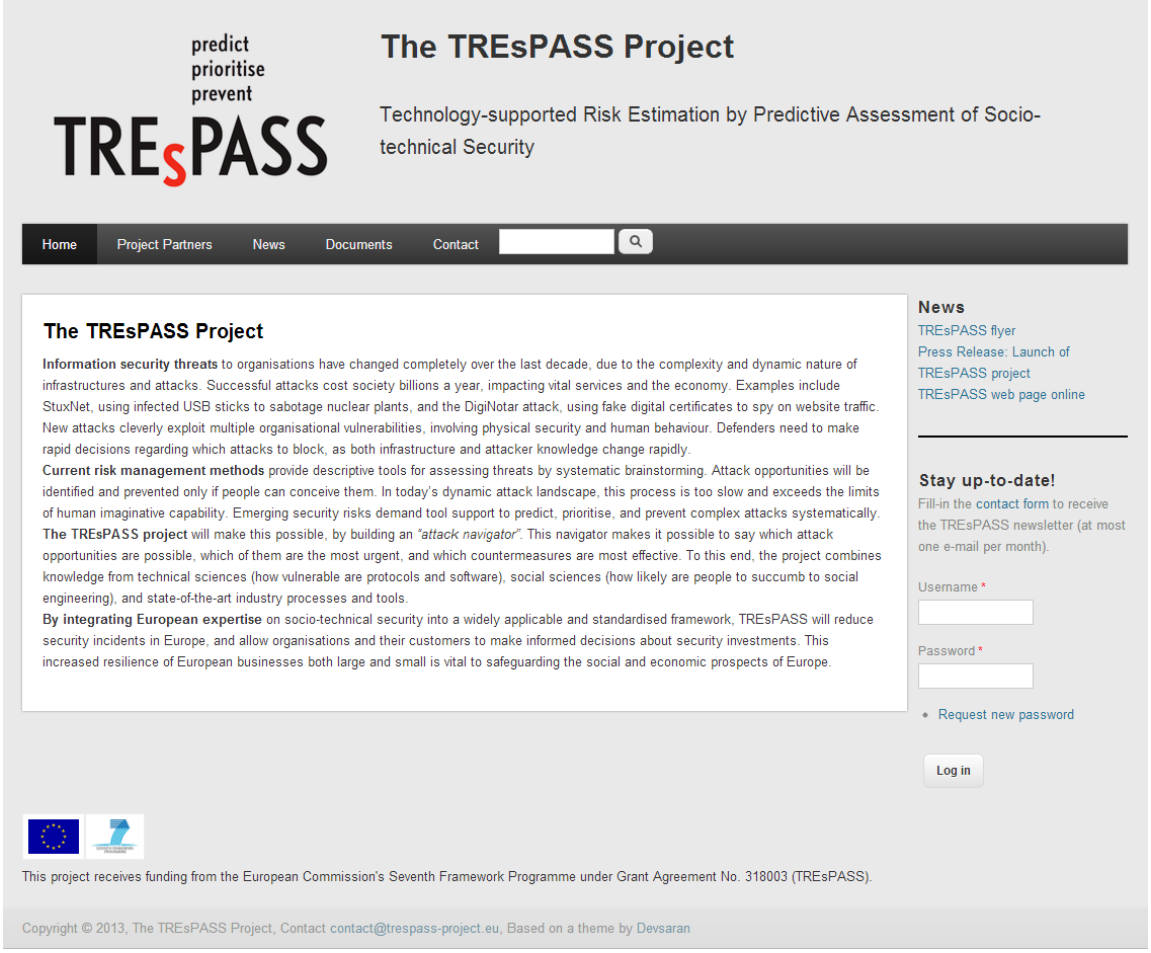

Figure 2.1: Home page of website

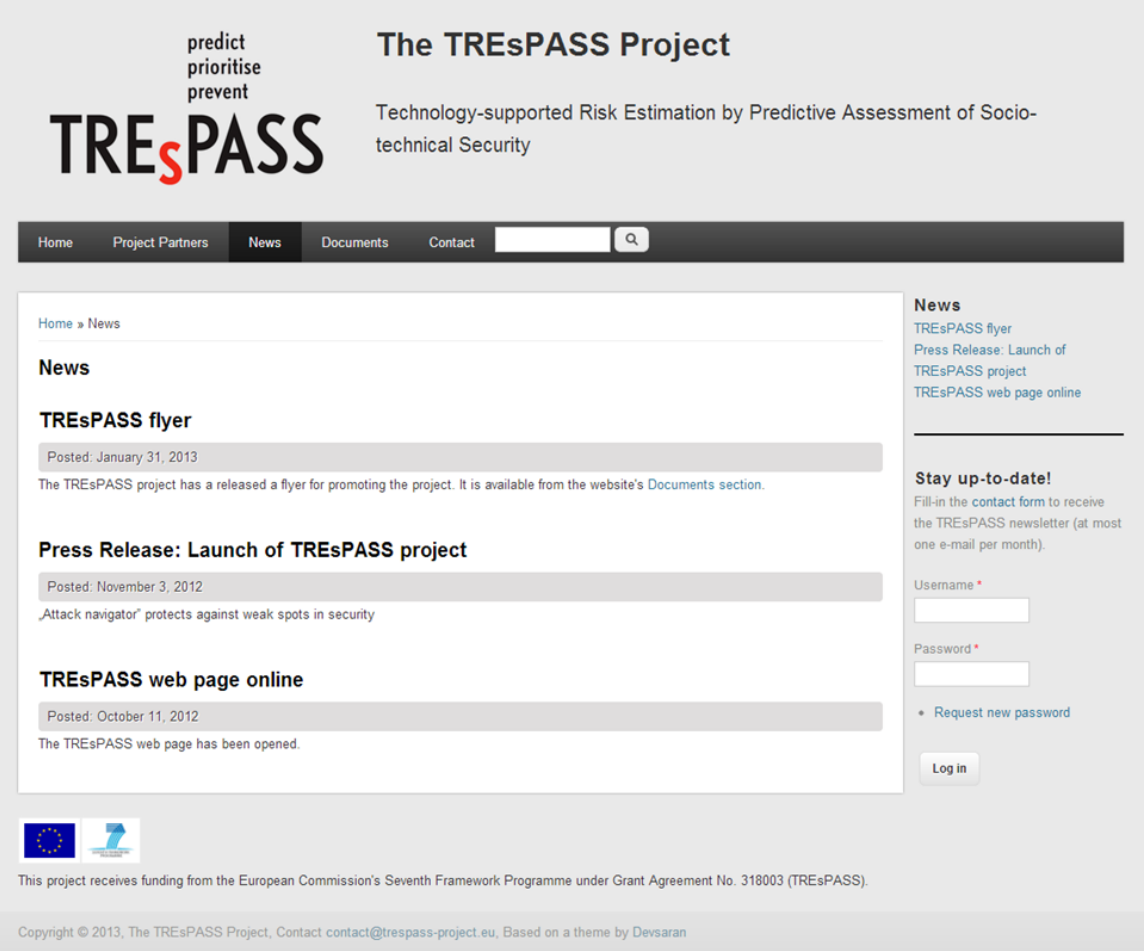

Figure 2.2: News page of website

3 Brochure

The brochure will be distributed at conferences. It is available in the following URL: https://www.trespass-project.eu/Documents

predict
prioritise
prevent

TREsPASS

Technology-Supported
Risk
Estimation by
Predictive
Assessment of
Socio-Technical
Security

Information security threats to organisations have changed completely over the last decade, due to the complexity and dynamic nature of infrastructures and attacks. Successful attacks cost society billions a year, impacting vital services and the economy. Examples include StuxNet, using infected USB sticks to sabotage nuclear plants, and the DigiNotar attack, using fake digital certificates to spy on website traffic. New attacks cleverly exploit multiple organisational vulnerabilities, involving physical security and human behaviour. Defenders need to make rapid decisions regarding which attacks to block, as both infrastructure and attacker knowledge change rapidly.

Current risk management methods provide descriptive tools for assessing threats by systematic brainstorming. Attack opportunities will be identified and prevented only if people can envisage them. In today's dynamic attack landscape, this process is too slow and exceeds the limits of human imaginative capability. Emerging security risks demand tool support to predict, prioritise, and prevent complex attacks systematically.

The TREsPASS project will develop methods and tools to analyse and visualise information security risks in dynamic organisations, as well as possible countermeasures. An "attack navigator" will be built to identify which attack opportunities are possible and most pressing, and which countermeasures are most effective. To this end, the project combines knowledge from technical sciences (how vulnerable protocols and software are), social sciences (how likely people are to succumb to social engineering), and state-of-the-art industry processes and tools.

By integrating European expertise on socio-technical security into a widely applicable and standardised framework, TREsPASS will reduce security incidents in Europe, and allow organisations and their customers to make informed decisions about security investments. This increased resilience of European businesses both large and small is vital to safeguarding the social and economic prospects of Europe.

The TREsPASS consortium comprises the entire value chain, including academic researchers in the social and the technical sciences, researchers and practitioners from large multinational companies, and developers and practitioners from SMEs. TREsPASS is coordinated by Prof. Pieter Hartel of the University of Twente. The other partners in the project are the Technical University of Denmark, Cybernetica (Estonia), GMV Spain, GMV Portugal, Royal Holloway University of London (United Kingdom), itrust Consulting (Luxembourg), Goethe University Frankfurt (Germany), IBM Research – Zurich (Switzerland), Delft University of Technology (Netherlands), Hamburg University of Technology (Germany), the University of Luxembourg (Luxembourg), Aalborg University (Denmark), Consult Hyperion (UK), BizzDesign (Netherlands), Deloitte (Netherlands), and Lust (Netherlands).

SEVENTH FRAMEWORK PROGRAMME

European Commission

This project receives funding from the European Commission's Seventh Framework Programme under Grant Agreement No. 318003 (TREsPASS).

For further information:
www.trespass-project.eu
contact@trespass-project.eu

January 2013

Figure 3.1: Brochure

4 Powerpoint Templates

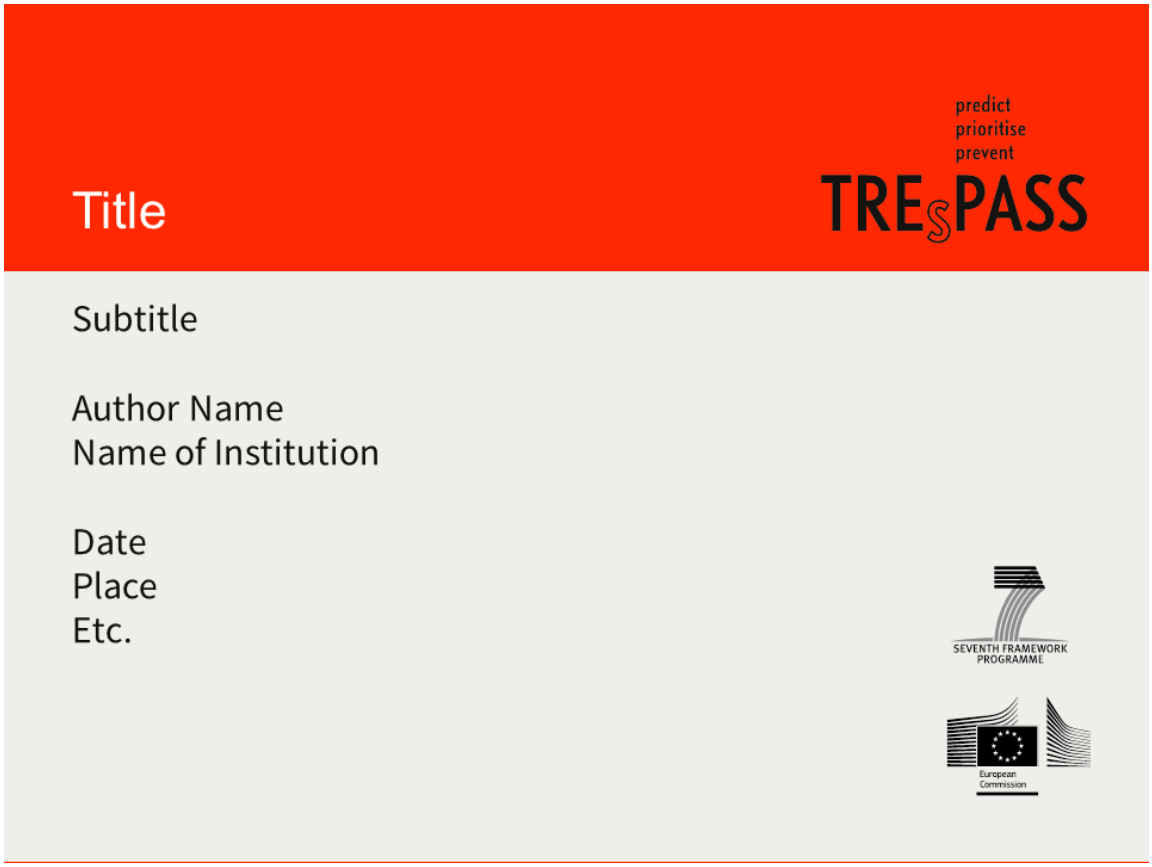

Figure 4.1: Powerpoint template - version 1

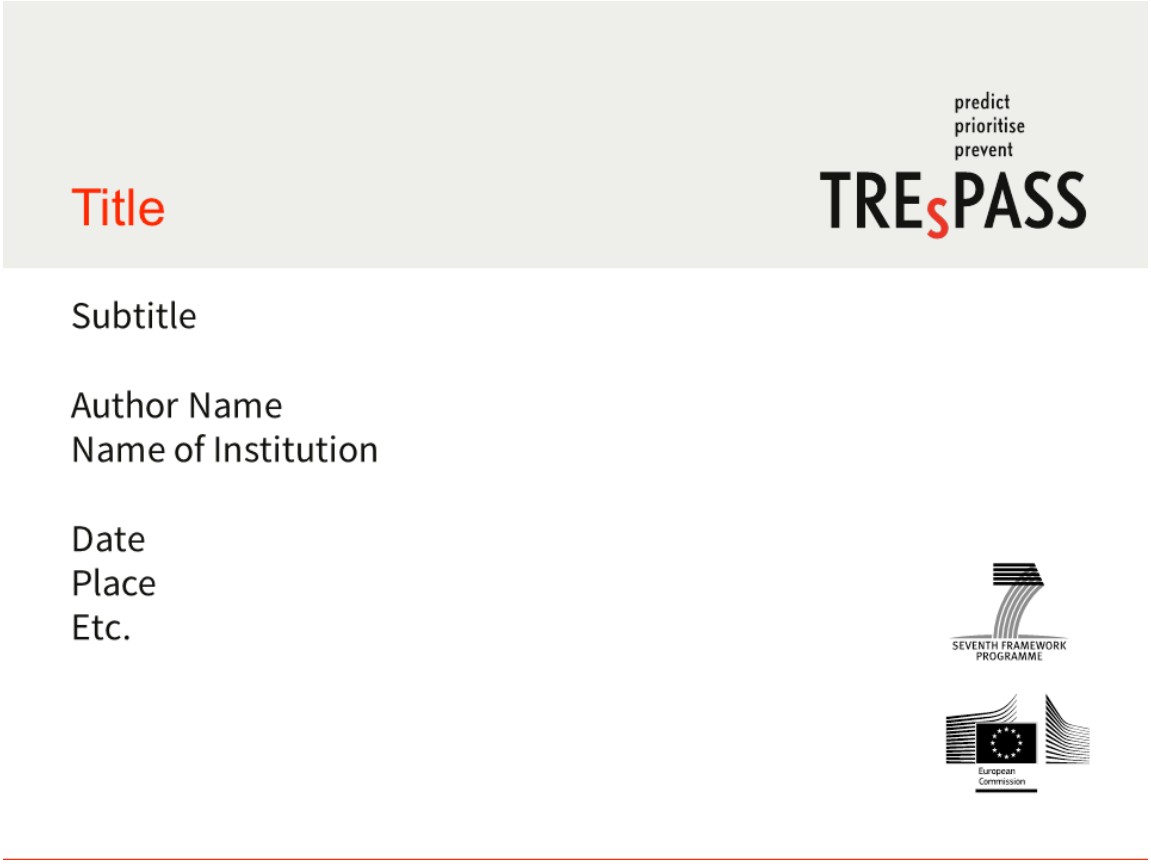

Figure 4.2: Powerpoint template - version 2

5 Press Releases

5.1 University of Twente

A press release was issued and its text was posted on the website on the following URL: https://www.trespass-project.eu/node/29

Human behaviour key in protecting information assets.

'Attack navigator' protects against weak spots in security.

An information infrastructure may be protected by the best technical means possible, but in the end it is often human behaviour that leads to unwanted intrusion or to the theft of information. By themselves, technical solutions will not solve these problems. That's why universities and companies all over Europe are getting involved in the TREsPASS project, which makes specific allowance for the human dimension. The aim is to develop a smart 'attack navigator', which will trace potential weak points within an organization or a given infrastructure. The 13.5 million euro project, which is being led by the University of Twente in the Netherlands, starts on 1 November.

Everyone is familiar with the yellow 'Post-it' memos, showing login details, that are often found stuck to computer monitors. The same goes for USB sticks found in car parks. However, few grasp the real impact of such actions on an organization's business or brand. Both may eventually lead to data theft, not as a result of any technical failure, but as a result of the vagaries of human behaviour. The TREsPASS project's 'attack navigator' combines technical and human aspects of security to identify weak points in organizations and their infrastructure. The tool can then help users to select the most effective countermeasures. To this end, the project combines knowledge from the technical sciences (how vulnerable are protocols and software?) and social sciences (how vulnerable are patterns of human behaviour and why?), as well as state-of-the-art industry processes and tools. Visualizing this information in a sufficiently expressive way is one of the challenges facing this project.

University of Twente The four-year project entitled "Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security" (TREsPASS) pools expertise from the University of Twente with that of 16 partners. The project coordinator is Prof. Pieter Hartel of the Distributed and Embedded Security Group. Various other technical groups from the University of Twente are also involved. These include Prof. Jaco van de Pol's Formal Methods and Tools and Prof. Roel Wieringa's Information Systems. Professor Marianne Junger's Social Risks and Safety Studies group will focus on the human aspects.

The University of Twente's share of the project budget is 3.3 million euros, of which 2.6 million is funded by the EU.

The University of Twente's partners in TREsPASS are the Technical University of Denmark, Cybernetica (Estonia), GMV Spain, GMV Portugal, Royal Holloway University of London (United Kingdom), itrust Consulting (Luxembourg), Goethe University Frankfurt (Germany), IBM Research Zürich (Switzerland), Delft University of Technology (Netherlands), Hamburg University of Technology (Germany), the University of Luxembourg (Luxembourg), Aalborg University (Denmark), Consult Hyperion (UK), BizzDesign (Netherlands), Deloitte (Netherlands), and Lust (Netherlands).

The TREsPASS project is funded by the European Union, as part of the FP7 Framework Programme.

The project website is: www.trespass-project.eu

Press contact: Wiebe van der Veen, tel +3153 4894244, or +31612185692

5.2 GMV Innovating Solutions

GMV participa no projeto TREsPASS para integrar o comportamento humano na segurança das empresas e das organizações públicas.

No âmbito dos programas de I&DT da Comissão Europeia, a GMV Portugal está a participar no projeto TREsPASS, no sentido de melhorar a segurança das empresas e das suas infraestruturas IT integrando os aspetos sociais na gestão do risco, nas infraestruturas IT e nos sistemas de informação. Lisboa, 17 de Janeiro de 2013 – A GMV, empresa tecnológica Portuguesa no sector das Tecnologias de Informação e Comunicação, acaba de anunciar a participação durante quatro anos no projeto TREsPASS como parte do FP7 Framework Programme da União Europeia. O nome do projeto TREsPASS é o acrónimo de "Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security". As infraestruturas de informação podem ser protegidas o melhor possível, mas no final é o comportamento humano que permite as intrusões não autorizadas ou o roubo de informação. Por si próprias, as soluções técnicas não resolvem esses problemas. É por isso que várias universidades e empresas na Europa estão a trabalhar no projeto TREsPASS que presta atenção específica para à dimensão humana. O objetivo é desenvolver um "Attack navigator" inteligente que rastreie pontos potencialmente fracos dentro de uma organização ou numa infraestrutura. O projeto tem um orçamento de 13,5 M€ é liderado pela universidade de Twente na Holanda.

Todas as pessoas estão familiarizadas com os Post-it amarelos, mostrando os detalhes das passwords que frequentemente são encontrados nos ecrãs dos computadores. Acontece a mesma coisa com os USB sticks encontrados nos parques de estacionamento. Contudo, poucas pessoas compreendem o impacto real destas ações no negócio das empresas ou nas marcas. Ambas podem eventualmente levar ao roubo de informação, não como resultado duma falha técnica, mas sim dos caprichos do comportamento humano. O "Attack navigator" do projeto TREsPASS combina os aspetos técnicos e humanos da

segurança para identificar pontos fracos nas organizações e nas suas infraestruturas. Deste modo, a ferramenta pode ajudar os utilizadores a selecionar as contramedidas mais efetivas. Para este fim, o projeto combina o conhecimento das ciências técnicas (quão vulneráveis são os protocolos e o software?) e das ciências sociais (quão vulneráveis são os padrões do comportamento humano e porquê?), assim como os processos e ferramentas do estado da arte da indústria. Visualizar esta informação de uma forma suficientemente expressiva é um dos desafios deste projeto. O projeto TREsPASS é financiado pela Comissão Europeia, como parte do 7th Framework Programme.

Descubra mais em http://www.trespass-project.eu/

Sobre a GMV Com receitas anuais superiores a 115 milhões de euros e uma equipa superior a 1100 profissionais (cerca de 80 baseados em Portugal), a GMV é um grupo tecnológico internacional fundado em 1984 que atua nas áreas Aeroespacial, da Segurança e Defesa, dos Transportes, da Saúde, das Telecomunicações e das TIC. A estratégia de crescimento da empresa baseia-se na inovação contínua, dedicando cerca de 10Controlo de Satélites, a terceira empresa europeia por volume de participação no Sistema de navegação por satélite Galileo, e o primeiro fornecedor Ibérico de sistemas telemáticos para o transporte público. Em termos de vigilância marítima, a GMV instalou as redes AIS da Madeira e dos Açores, é um dos principais fornecedores da EMSA, desenvolve software para o IPTM, e participa em vários projetos de monitorização de navios por satélite com a ESA. Por outro lado, a GMV fornece soluções de segurança para grandes empresas do setor financeiro, seguradoras, de telecomunicações, utilities, saúde e administração pública.

Para mais informações visite www.gmv.com.pt

Contactos de Imprensa
Andreia Fernandes
Consultora de Comunicação
OUTMarketing – Outsourcing de Marketing em TI
Telefone: +351 21 099 51 01
Telemóvel: +351 91 785 74 78
E-mail: andreia.fernandes@outmarketing.pt

Marketing Portugal
Telefone : +351 21 382 93 66
E-mail : marketing.portugal@gmv.com

6 Press Coverage

There was press coverage in printed form in the Dutch newsletter TW TechnischWeekBlad from (17/11/2012, volume 43, issue 46, pg 1).

The following are the URLs of online press coverage up until the 31st of January 2013.

TW TechnischWeekBlad (18 Nov 2012)
http://www.technischweekblad.nl/attack-navigator-beschermt-bedrijfsgegevens.296287.lynkx
Computerworld (25 Jan 2013)
http://www.computerworld.com.pt/2013/01/25/projecto-europeu-procura-pontos-fracos-nas-organizacoes/
Fibra (23 Jan 2013)
http://www.fibra.pt/empresas/6140-gmv-portugal-em-projeto-europeu-sobre-seguranca-das-empresas.html
Sciencedaily (5 Nov 2012)
http://www.sciencedaily.com/releases/2012/11/121105081457.htm
Leak Business (22 Jan 2013)
http://business.leak.pt/gmv-portugal-contribui-para-a-seguranca-de-empresas-e-organizacoes-publicas/
Infosecurity (11 Nov 2012)
http://www.infosecurity.net/Nieuws/78801/TREsPASS-ontwikkelt--attack-navigator-
C2W (18 Nov 2012)
http://www.c2w.nl/attack-navigator-beschermt-bedrijfsgegevens.296287.lynkx