Approccio europeo alla Software Vulnerability Disclosure

GIANLUCA VARISCO
Team per la Trasformazione Digitale
Governo Italiano

CHI SONO

Team per la Trasformazione Digitale

Coordinated Vulnerability Disclosure (CVD)

A cosa serve?

Definisce una modalità
per riportare le vulnerabilità,
lasciando al ricevente il tempo
necessario per individuare
e applicare le opportune contromisure,
prima di renderle pubbliche.

Benefici

La tempestività nel risolvere le falle risulta cruciale per ridurre la finestra temporale in cui i software sono esposti a soggetti malevoli.

Ruolo del Team

Crediamo fermamente nella Coordinated Vulnerability Disclosure (CVD) come uno degli strumenti principali per fare un uso positivo e controllato delle fortissime conoscenze della comunità di ethical hacker italiane e internazionali.


È un duro lavoro
di squadra

CEPS Task Force on «SW Vulnerability Disclosure in Europe»

PERCHÉ?

I ricercatori di sicurezza nell'Unione Europea necessitano di:

- una maggiore chiarezza giuridica
- standard consistenti

28 stati membri
28 situazioni disomogenee

Esempio: Ungheria

The discovery was first made when a Hungarian teenager figured out that ticket prices could easily be altered by simply using the browser's Element Inspector (viewable by pressing F12 on the keyboard) and changing the ticket price on the website. As the software had no server-side checks, it took whatever value was on the user's end as the correct price for tickets.

The case has revealed that a widely accepted practice of ethical hacking does not exist in Hungary, and partly perhaps due to lack of such, a true consensus has also not evolved, yet. It is time to start the social and professional dialogue addressing "ethical hacking" in Hungary, too, and to establish the relevant legal and regulatory frameworks for the activity. Pursuing this objective, T-Systems shall introduce some relevant initiatives ("bug bounty") in the near future.

Hungarian hacker arrested for pressing F12

John Biggs @johnbiggs / Jul 25, 2017 Comment

The Budapest Transport Authority (BKK, in Hungarian) recently launched an online payment system with the help of a T-Systems Hungary, Deutsche Telekom's consulting arm. The system, which took three months to build, was supposed to be installed in time for the FINA world championships in Budapest. The software, not unexpectedly for such a project, was full of bugs including the discovery of an administration screen with with a password set to "adminadmin."

Last week, GovCERT, Hungary's national cyber security institution operating under the national special services released an ad emphasizing that ethical hackers could report any security flaws to the government, anonymously if they want. If they want to disclose personal data, the agency will handle it confidentially. Furthermore, the mayor of Budapest announced that T-Systems will have to correct the app they delivered to BKK, on their own expense.

Altri esempi

Zack Whittaker
@zackwhittaker

Following

A expert letter signed by over 50 security experts and advocates, including reporters, urge support for security researchers and reporters in their work, and decry those who oppose research and discussion of privacy and security risks. cdt.org/insight/expert …

The ability of researchers to find and responsibly report vulnerabilities is more important today now that traditionally unconnected devices are being connected to the Internet and more of people's lives are mediated by data, computation, and networking. Compromised systems and devices have been used to launch attacks all over the world. Vulnerability research, discovery, and disclosure are critical features of the modern digital society; the US National Institute of Standards and Technology has recognized in its Cybersecurity Framework that vulnerability disclosure is an important aspect of any effective cybersecurity program.

Security researchers who search for vulnerabilities often find themselves in areas where laws or regulations forbid or hinder tinkering with devices and software. They are at particular risk where copyright is involved or where they publicly report their discoveries.

In the US, security researchers and reporters have recently been targeted by unwarranted and opportunistic legal threats and lawsuits.

The most recent cases include *Keeper v. Goodin*[1] and *River City Media v. Kromtech*[2]; in the first case, a reporter was sued for reporting on the details of a vulnerability, and in the second case a security researcher is being sued for investigating a publicly accessible spam server. These lawsuits not only endanger a free and open press but risk a "chilling effect" towards research designed to improve cybersecurity. Security researchers hesitate to report vulnerabilities and weaknesses to companies for fear of facing legal retribution; these chilling effects invite the release of anonymous, public zero-day research instead of coordinated disclosure.

We urge support for security researchers and reporters in their work, and decry those who oppose research and discussion of privacy and security risks. Harming these efforts harms us all.

2:40 PM - 10 Apr 2018

Researcher informs drone maker DJI about bugs, gets called a 'hacker' and threatened

by ABHIMANYU GHOSHAL — 6 months ago in SECURITY

Lawsuits threaten infosec research — just when we need it most

Security researchers and reporters have something in common: both hold the powerful accountable. But doing so has painted a target on their backs — and looming threats of legal action and lawsuits have many concerned.

By Zack Whittaker for Zero Day | February 19, 2018 -- 13:00 GMT (13:00 GMT) | Topic: Security

Partecipanti

Chair: Marietje Schaake, Member of the European Parliament

Coordinator: Lorenzo Pupillo, Associate Senior Research Fellow, CEPS

Rapporteurs: Afonso Ferreira, Directeur de Recherche CNRS and Gianluca Varisco, Cybersecurity Expert, Italian Digital Transformation Team

Research Assistant: Antonella Zarra, CEPS

Advisory Board

Ross Anderson, Professor of Security Engineering at Computer Laboratory, University of Cambridge

Andriani Ferti, Senior Associate Karatzas & Partners Law Firm

Allan Friedman, Cybersecurity Director, US National Telecommunications and Information Administration

Tim Watson, Director of the WMG Cyber Security Centre, University of Warwick

Partecipanti

Companies and European Organisations

Jochai Ben-Avie, Senior Global Policy Manager, Mozilla

Mariano Cunietti, Chief Technology Officer, Enter

Jeroen van der Ham, National Cyber Security Centre, The Netherlands

Lise Fuhr, Director General, European Telecommunications Network Operators

Caroline Greer, Head of European Public Policy, Cloudflare

Evgeny Grigorenko, Head of Public Affairs, Europe, Kaspersky Lab

Baiba Kaskina, CERT Latvia and Chair TF-CSIRT

Stephane Lenco, Chief Information Security Officer, Airbus

Jan Neutz, Cybersecurity Policy Director, EMEA, Microsoft

Jan-Jacque Sahel, Vice President for Global Stakeholder Engagement, Europe and Civil Society, ICANN

Corinna Schulze, Director, EU Government Relations, Global Corporate Affairs, SAP

Mark Smitham, Senior Manager, Microsoft

Partecipanti

European Institutions

Laurent Beslay, Project Leader, Joint Research Centre, European Commission

Monika Kopcheva, Political Administrator, Council of the European Union

Aristotelis Tzafalias, Policy Officer, Cybersecurity and Digital Privacy, European Commission

Claudia Warken, Policy Officer, DG Home Affairs, European Commission

Mathias Vermeulen, Policy Advisor to MEP Marietje Schaake, European Parliament

Civil Society

Jens-Henrik Jeppesen, European Policy Director, Center for Democracy and Technology

Lucie Krahulcova, EU Policy Associate, Access Now

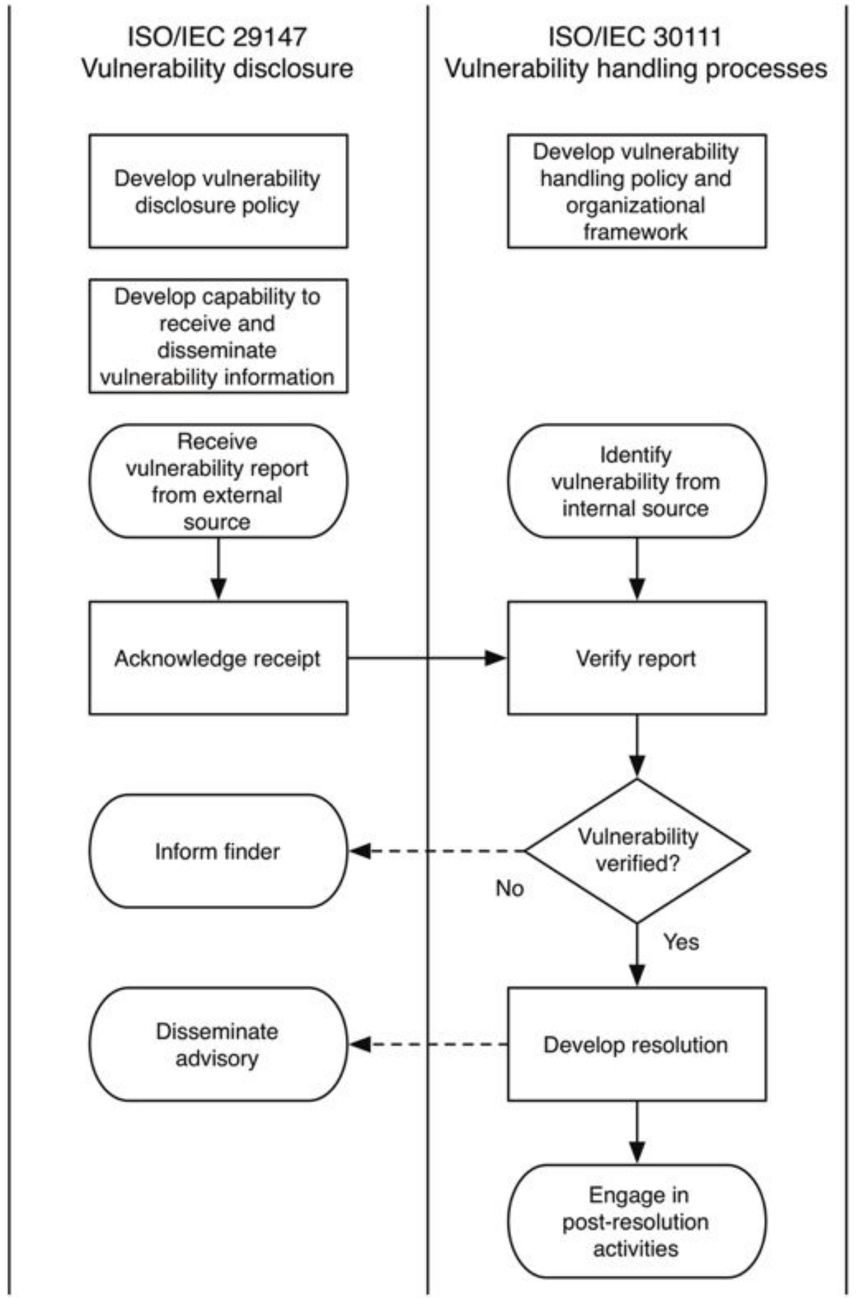
Academia

Stefano Fantin, Legal Researcher, Centre for IT and IP Law, Katholieke Universiteit Leuven

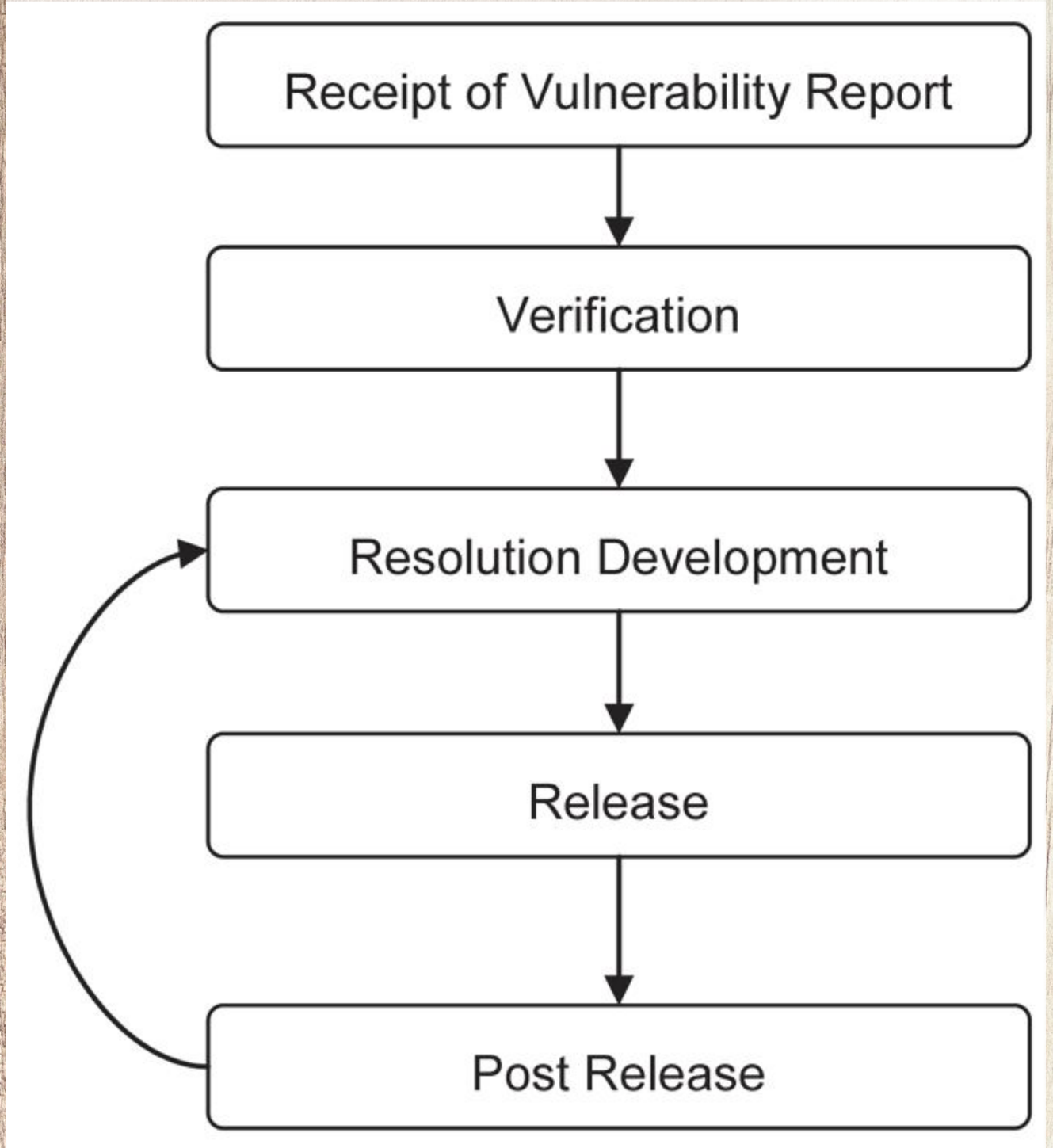
Extra -EU Organisations

Uchiyama Takayuki, CERT Japan

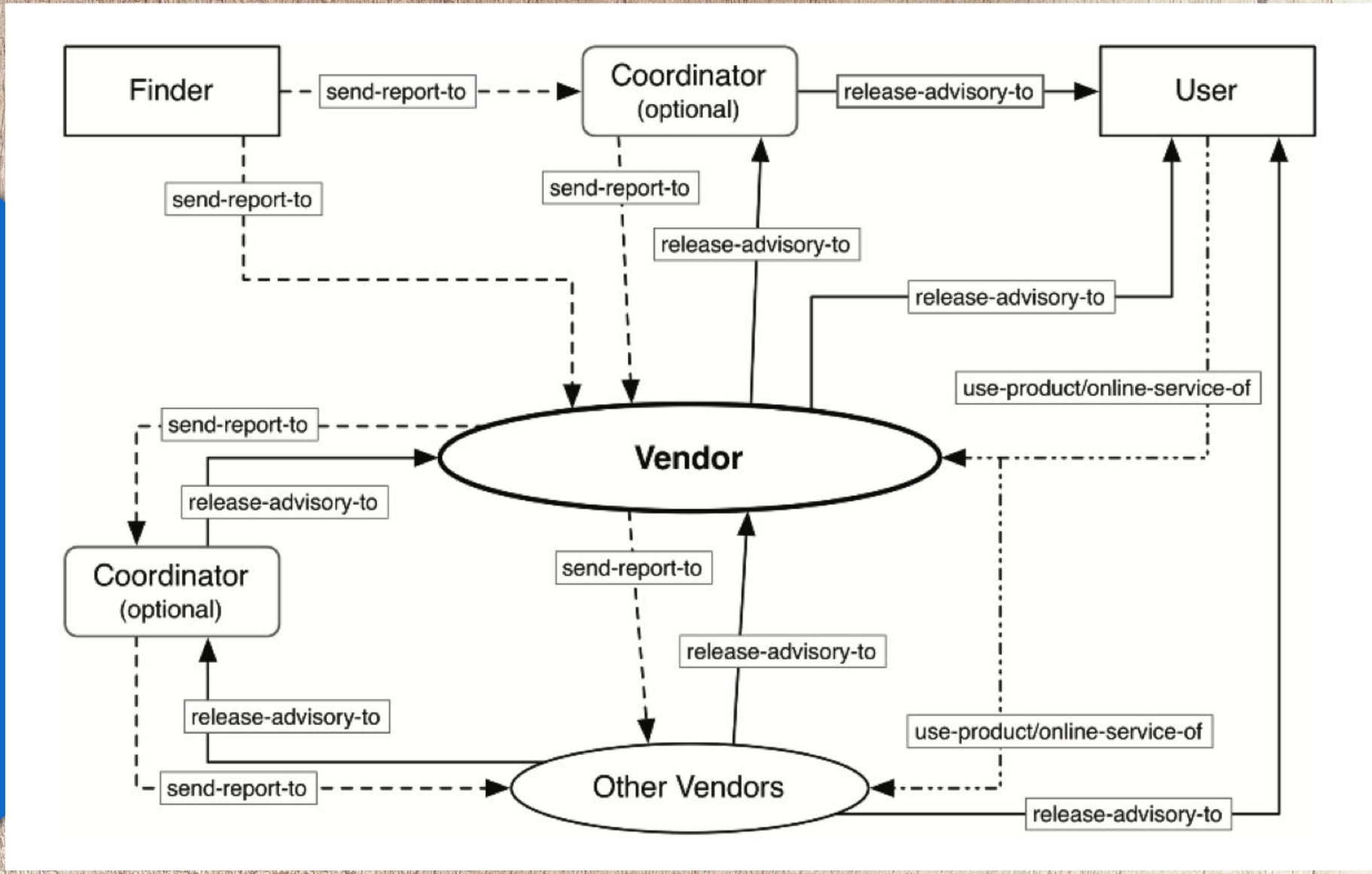
ISO/IEC 29147 e ISO/IEC 30111



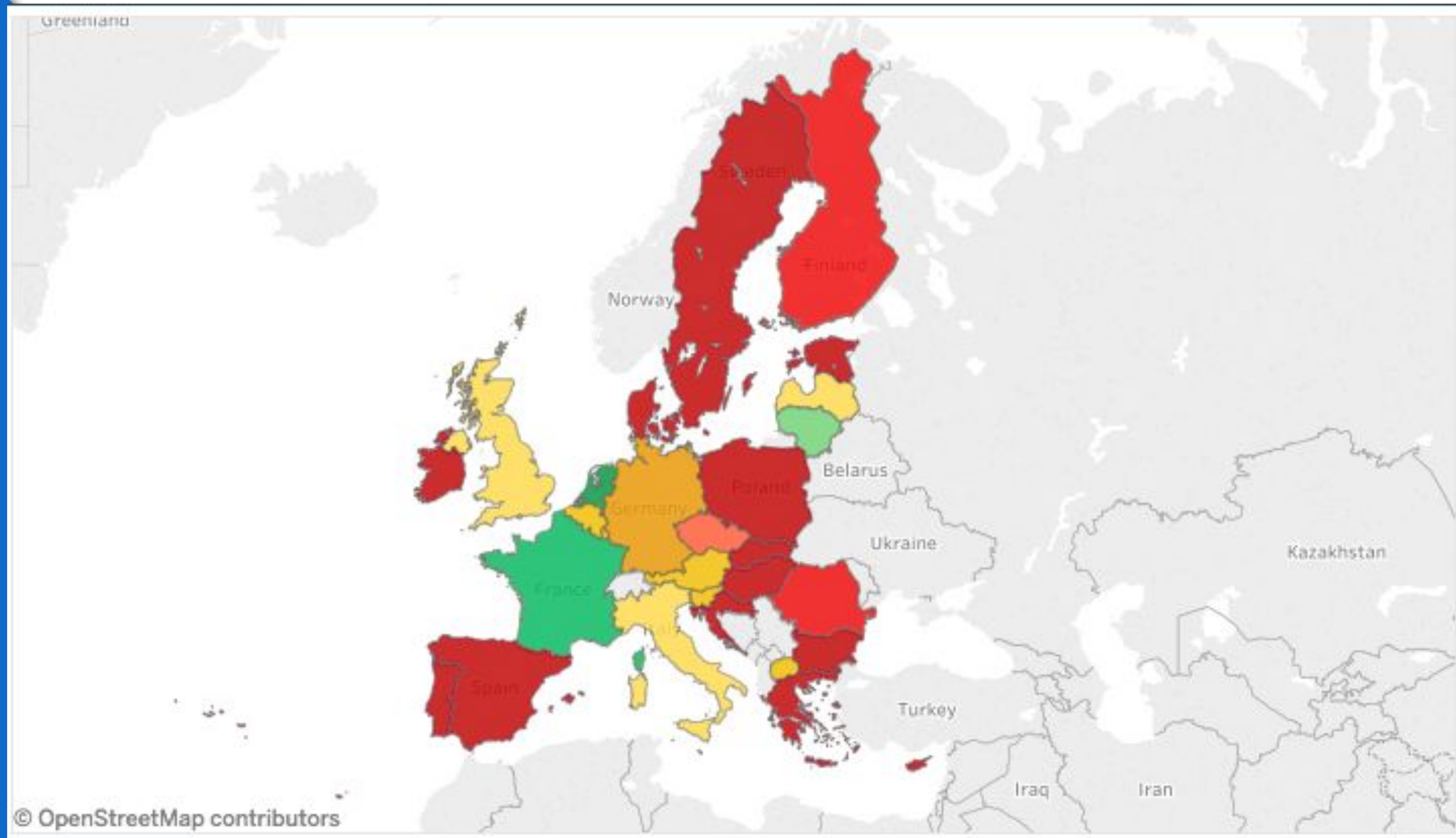
Summary vulnerability disclosure process

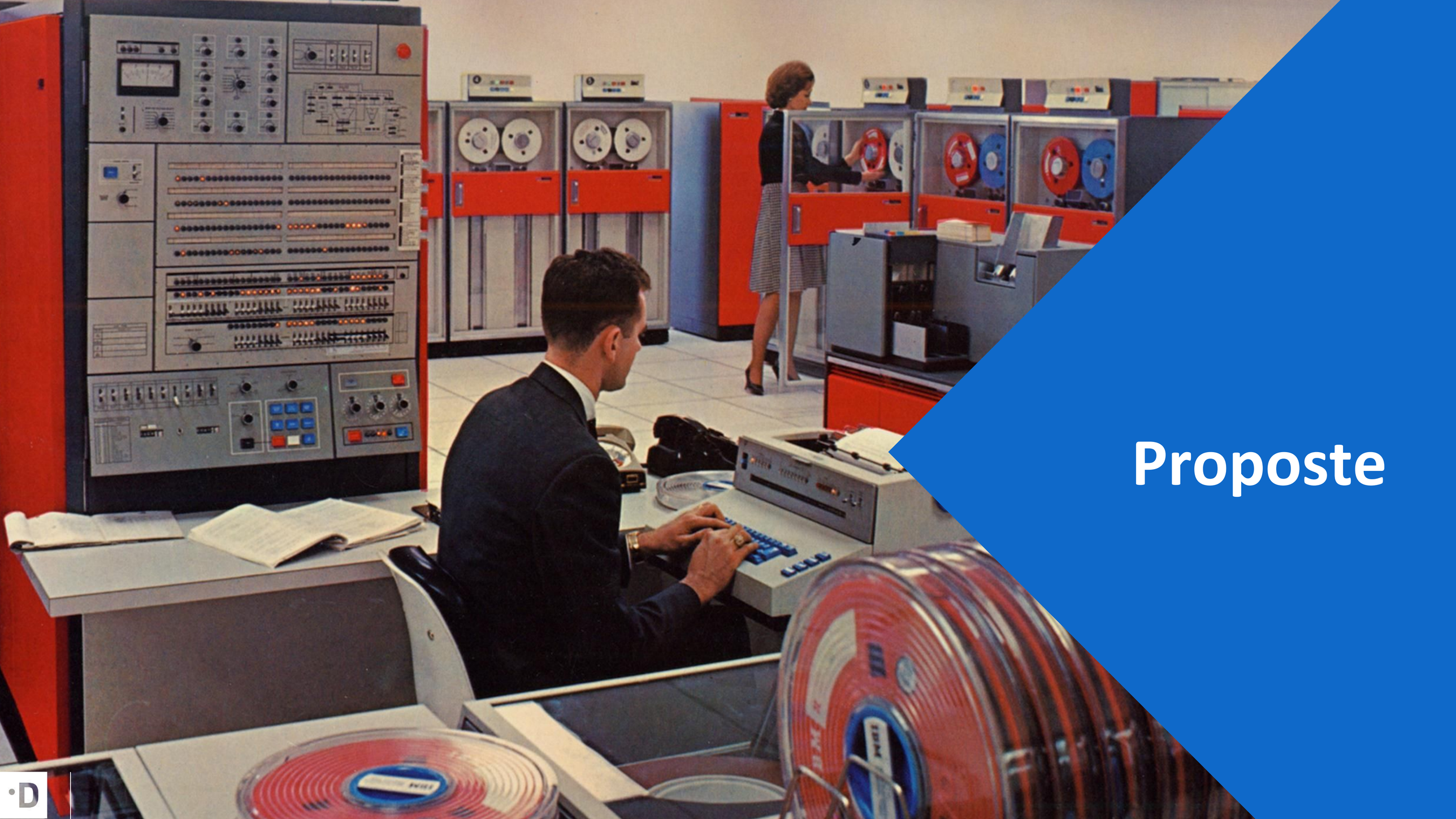


Vulnerability information exchange



Mappatura


Greenland
Sweden
Finland
Norway
Belarus
Poland
Germany
Ukraine
Kazakhstan
France
Spain
Turkey
Iraq
Iran
© OpenStreetMap contributors



Proposte

CVD Policy

European-level framework complemented by national legislation

Amending national legislation

Member states should amend their national legislation bearing on CVD, using the framework on CVD introduced in the Netherlands as a model.

EU Legislation

Amending Directive 2013/40/EU on attacks against information systems (the "EU cybercrime Directive") to support CVD

EU Legislation

Protection of security researchers

EU Legislation

Incentives for security researchers

EU Legislation

Cybersecurity Act:
ENISA can contribute to the harmonised development of CVD in the EU by having its mandate amended.

Report finale previsto per Giugno 2018

Grazie!

Domande?

Seguici su:

teamdigitale.governo.it
pianotriennale-ict.italia.it

@gvarisco, @teamdigitaleIT

@gvarisco, @team-per-la-trasformazione-digitale

@company/teamdigitale