ENISA Cyber Europe 2014

Media Coverage

1.1 English Coverage

- Businesses participate in 'biggest ever' cyber security exercise, By Staff, Out-Law.com, 31 October 2014
- Working together helps build confidence, By Nathalie Steiwer, Europolitics, 31 October 2014 (*full text below*)
- Hundreds of companies face 2,000 cyber-attacks in EU exercise, By Doug Drinkwater, SC Magazine, 31 October 2014

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

HOME | NEWS | PRODUCTS | WHITEPAPERS | EVENTS | SC AWARD

SC Magazine UK > News > Hundreds of companies face 2,000 cyber-attacks in EU exercise

Doug Drinkwater, Senior Reporter

Follow @DougDrinkwater

October 31, 2014

Hundreds of companies face 2,000 cyber-attacks in EU exercise

Share this article:

The European Network and Information Security Agency (ENISA) conducted a 24-hour cyber-exercise in which more than 200 organisations from 25 EU member states faced virtual cyber-attacks from white hat hackers yesterday.

Cyber Europe 2014 targeted security agencies, ministries, telecoms, energy companies, financial institutions and internet service providers (ISPs) in a 24-hour exercise where almost all EU member states (except Belgium, Lithuania and Malta) tested their cyber-defence procedures against as many as 2,000 real-life attacks. These attacks included DDoS and web defacement attacks, data exfiltration and cyber-attacks against critical infrastructure.

Approximately 400 cyber-security professionals were involved in the exercise, which also involved national CERTs (Computer Emergency Response Teams). ENISA is expected to launch an in-depth report on the results from the exercise later in the year.

European Commission VP Neelie Kroes said that this kind of education is required in the face of an emerging cyber threat landscape.

"The sophistication and volume of cyber-attacks are increasing every day. They cannot be countered if individual states work alone or just a handful of them act together," she said in a statement.

Hundreds of companies face 2,000 cyber-attacks in EU exercise

"I'm pleased that EU and member states are working with the EU institutions, with ENISA bringing them together. Only this kind of common effort will help keep today's economy and society protected."

ENISA executive director, Professor Udo Helmbrecht, added in a statement: "Five years ago there were no procedures to drive cooperation during a cyber-crisis between EU member states. Today we have the procedures in place collectively to mitigate a cyber-crisis on European level," said.

"The outcome of today's exercise will tell us where we stand and identify the next steps to take in order to keep improving."

Brian Honan, managing director and lead consultant at BH Consulting, said that it could prove useful for national CERTS.

"These tests are very useful in that they not only allow CERTs to practice their technical capabilities in the face of certain types of attacks, but more importantly they establish and reinforce communication and cooperation across CERTs in many different countries in the EU," he told *SCMagazineUK.com*.

"One of the key elements in dealing with a major cyber-attack is being able to call on other CERTs to help deal with the attack. This may be in the form of dealing with the suspected source of attacks within their jurisdiction or providing resources and expertise in areas that your own team may not be strong. Knowing which CERT to contact, how to contact them, and who the key people are within each CERT are vital to ensure quick response and resolution to an attack. Running regular exercises can help establish and maintain those lines of communications."

He added: "The other advantage it provides is that it can help establish and maintain a base level of capabilities across all CERTs. As with all aspects of cyber-security, some teams are more proficient than others. It is better to identify those teams that have deficiencies in certain areas during an exercise and address those weaknesses, rather than discover them during a real event.

Adrian Culley, a former Scotland Yard cyber-crime detective and now cyber-security consultant, said that the exercise – while laudable – was a big ask in just 24 hours.

"The aims of the exercise are laudable, however the scope seems somewhat immense to be effectively and efficiently covered in a single day," he said in an email to *SC*.

"For such exercises to be truly meaningful they must have a tangible technical aspect ie real attacks on real systems, even if this is contained in an air-gapped training system. There is limited scope for meaningful learning from a purely paper based table-top exercise in this arena."

This news coincides with a new set of guidelines being released aimed at improving inta-country cyber-sharing. The EU-Standard Operational Procedures (EU-SOPs) are designed to test how countries share operational information about cyber-threats.

-
- Europe runs largest cyber-security exercise to date, Tereza Putlarova, E&T, 31 October 2014

- Biggest cyber-threat 'from software failure, not crime', Ann Cahill, Irish Examiner, 31 October 2014
- European professionals discuss ways to promote cyber security, By Staff, Shanghai Daily, 31 October 2014
- Zero Day Weekly: CurrentC hacked, White House Breached, APT28 exposed, Verizon shamed, By Staff, ZDNet, 31 October 2014
- 200 Organization Take Part in Largest European Cybersecurity Exercise to Date, By Eduard Kovacs, Security Week, 30 October 2014
- EU carrying Out Biggest Ever Cybersecurity Exercise: Information Security Agency, By Staff, RIA Novosti, 30 October 2014
- BIGGEST THREAT to Europe's cybersecurity? Hint: not hacker, By Jennifer Baker and John Leyden, The Register, 30 October 2014 (*full text below*)

The Register®

Data Centre Software Networks **Security** Business Hardware Science Bootnotes Video Forums

SECURITY

BIGGEST THREAT to Europe's cybersecurity? Hint: not hackers

Largest EVER Europe-wide cybersecurity exercise

By Jennifer Baker and John Leyden, 30 Oct 2014 Follow 3,064 followers

6

Linux and AIX Bare-Metal Recovery Webinar

Forget cyber-espionage, cyber-warfare and cyber-terrorism. The biggest threat to Europe's infrastructure cybersecurity are power outages and poor communication.

On Thursday, ENISA (European Network and Information Security Agency) held its biggest ever cybersecurity exercise involving more than 200 organisations and 400 cyber-security professionals from 29 European countries.

Track

Log in

- EU Conducts its largest cybersecurity test, By Cory Bennett, The Hill, 30 October 2014
- Biggest ever cyber security exercise in Europe is underway, By Staff, Net-Security, 30 October 2014
- EU holds largest-ever cyber-security exercise, By Derek Gatopoulos, Associated Press, 30 October 2014

AP THE BIG STORY

EU holds largest-ever cyber-security exercise

By DEREK GATOPOULOS Oct. 30, 2014 1:06 PM EDT

0

2 photos

Udo Helmbrecht, the director of the European Network and Information Security Agency, speaks to the... Read more

ATHENS, Greece (AP) — The European Union on Thursday carried out its biggest exercise to prevent cyber-attacks on Europe's public utilities and communications networks.

The director of the European Network and Information Security Agency, Udo Helmbrecht, told The Associated Press that Thursday's one-day exercise involving 29 countries and 200 agencies dealt with attack scenarios against "critical infrastructure."

Helmbrecht said European countries were working to improve their coordination between national security agencies and to further standardize protective software and methods.

Examples of serious past incidents, he said, include a wave of cyber-attacks against Estonia in 2007 that severely affected the country's banks and government agencies, and the Stuxnet computer virus that was used to target energy and industrial sites in Iran.

"Now this malware is out in the world, so if you are a criminal you can re-engineer it and use it to attack a water supply, or a car manufacturing plant, or a government," said Helmbrecht, speaking in a windowless office in an EU building where part of the exercise is being held.

The EU agency, based in Iraklio, on the Greek island of Crete, says web-based attacks increased globally by nearly a quarter in 2013 from a year earlier, directed from an increasing number of countries.

"The sophistication and volume of cyber-attacks are increasing every day," Neelie Kroes, the EU Commission vice president, said in a statement Thursday.

"They cannot be countered if individual states work alone or just a handful of them act together."

The European cyber-security exercise is held every two years and the results of the current safety tests are due to be issued by the end of the year.

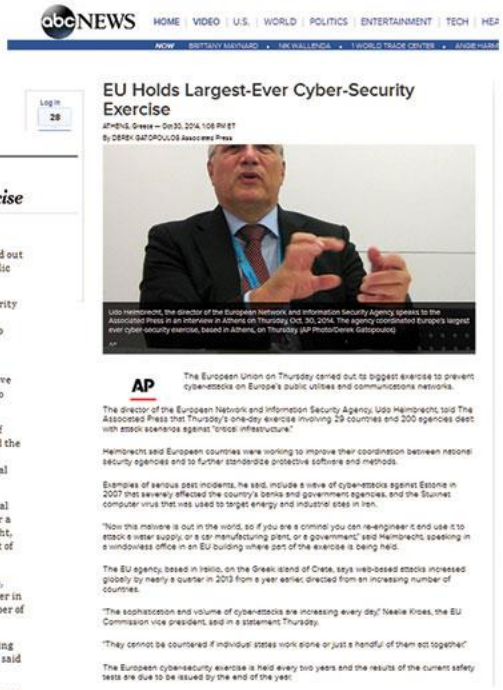
—

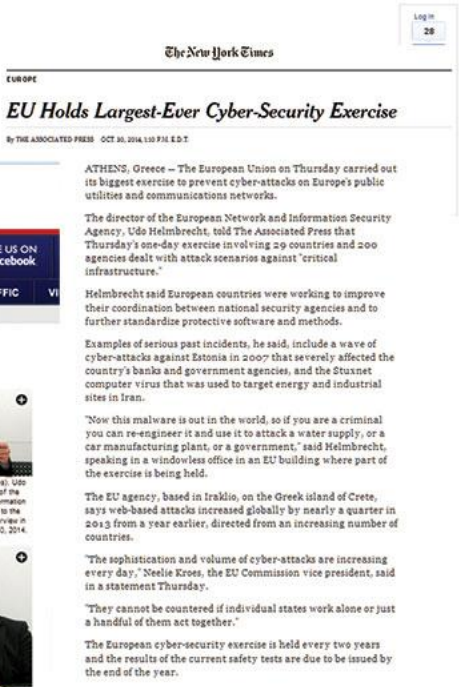
Online:

ENISA 2013 report on current and emerging cyber-threats: http://goo.gl/LtMSRw

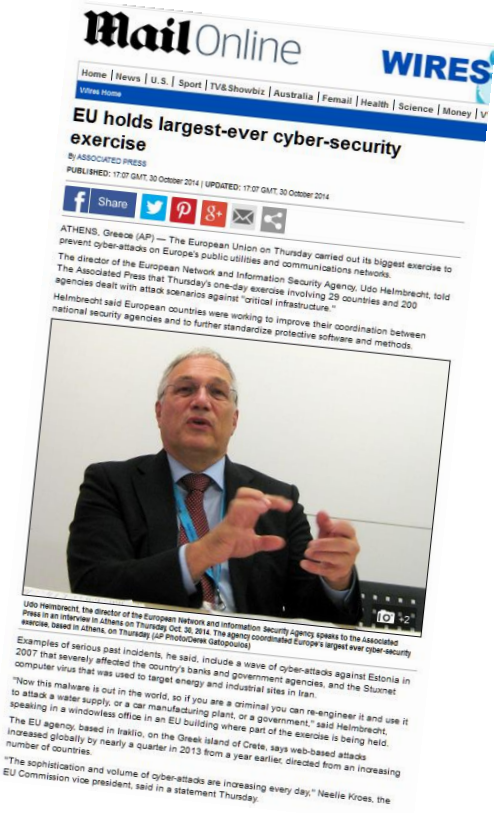
Syndicated by:

- New York Times
- ABC News
- FOX News





- Yahoo news
- Daily Mail
- Times of Israel
- Daily Reporter
- NDTV
- WHLT
- MyBroadBand
- The Garden Island
- Item Live
- US news



- Europe under massive virtual cyber attack, By Staff, EurActiv, 30 October 2014

EurActiv.com
EU News & policy debates, across languages
EN FR DE

România
OFICIAL BEC ora 17.00: 98,3% din secțiile de votare: 40,33% - Ponta, 30,44% -
OFICIAL BEC ora 11.00: 98,3% din secțiile de votare: 40,33% - Ponta, 30,44% -
OFICIAL BEC ora 11.00: 98,3% din secțiile de votare: 40,33% - Ponta, 30,44% -
OFICIAL BEC ora 09.00: 91,53% secții din Romania pana la ora 7:00
Rezultate partiale oficiale ale BEC dupa centralizarea a 56,21% din secțiile de vo

SECTIONS | NEWS | SPECIAL REPORTS | LINKSDOSSIERS | INTERVIEWS | OPINIONS

MORE IN THIS SECTION

- EU welcomes Orbán's scrapping of Internet tax
- Hungary will shelve Internet tax plan for now, Orbán says
- Outgoing Digital Commissioner: A lot more work is needed to clarify the 'right to be forgotten'
- Copyright reform: weak research will produce bad policy
- Berlin calls for EU-wide retention of PNR flight data

More

SECTION SUPPORTERS

allegro group

DIGITALEUROPE

EURACTORS

CCIA - Computer & Communications Industry Association
CISAC - International Confederation of Societies of Authors and Composers
ECTA - European Competitive Telecommunications Association
ESCAUX - Business IP Telephony
ETNO - The European Telecommunications Network Operators' Association
GSMA Europe - The European Interest Group of the GSM Association

Home › InfoSociety › News › Europe under massive virtual cyber attack

Europe under massive virtual cyber attack

Log in | Share 97 | Tweet 116 | Share 1

Published: 30/10/2014 - 12:38 | Updated: 03/11/2014 - 10:57 | 12

More than 200 organisations from 25 EU member states are under virtual cyber-attack today (30 October), as part of the continent's largest and most complex ever cyber security exercise.

Organised by the European Network and Information Security Agency (ENISA), Cyber Europe 2014 is targeting security agencies, ministries, telecoms and energy companies, financial institutions and internet service providers.

All EU member states except Belgium, Lithuania and Malta are testing their procedures and capabilities against realistic large-scale cyber-security scenarios. The reasons those countries have declined to participate are not known, but are "uncontroversial," according to ENISA sources.

More than 2000 separate cyber-incidents will be carried out, including denial of service attacks to online services, intelligence and media reports on cyber-attack operations, ambushes designed to change websites' appearances, and attacks on critical infrastructure such as energy or telecoms networks.

Report expected later this year

The exercise also represents the first large-scale test of new pan-European standard operating procedures to share information on cyber crisis.

Experts from ENISA will issue a report with key findings by the end of the year. "The exercise is becoming more important as threats increase (see background) and as the internet of things is becoming a reality," Steve Purser, head of operations department at ENISA told EurActiv.

Purser explained: "As people increasingly have a network of Internet-linked appliances controlling their domestic lives, the points of entry for cyber attack increase, and any point of weakness can be used to access key systems."

Organised by ENISA every two years, this year's exercise is the largest ever carried out and is likely to feed into the debate over the Commission's proposed cyber security directive, which is currently approaching the trilogue stage of negotiations between the European institutions in Brussels.

Italian presidency wants to complete cyber security directive

Italy believes that the directive can be agreed before its presidency finishes at the end of the year, but the scope of reporting obligations covered by any directive remains controversial.

The directive would oblige certain infrastructure-critical companies to report any cyber attacks, but the definition of what types of companies would be covered is controversial.

Some internet and software companies are resisting pressure to be forced to make reports, arguing that there could be unnecessary bureaucratic replication of reporting.

- EU launches largest ever European cyber security exercise, By Staff, Telecompaper, 30 October 2014

telecompaper

HOME : MOBILE & WIRELESS INTERNET GENERAL : FIXED : IT : BROADCAST

INTERNET

EU launches largest ever European cyber security exercise

Thursday 30 October 2014 | 11:43 CET | News

The EU's cyber security agency Enisa has launched what it has described as the largest and most complex cyber security exercise ever held in Europe. On 30 October more than 200 organisations and 400 cyber security professionals from 29 European countries will be testing their readiness to counter cyber attacks in a day-long simulation. Over 2,000 separate cyber-incidents will be dealt with, said Enisa, including denial of service attacks to online services, intelligence and media reports on cyber-attack operations, website defacements, ex-filtration of sensitive information, attacks on critical infrastructure such as energy or telecoms networks and the testing of EU cooperation and escalation procedures.

The public and private sector organisations taking part in the exercise include cyber security agencies, national computer emergency response teams, ministries, telecoms companies, energy companies, financial institutions and internet service providers. The ultimate aim of the exercise is to strengthen cyber crisis cooperation and enhance preparedness and response across Europe. "Five years ago there were no procedures to drive cooperation during a cyber-crisis between EU Member States. Today we have the procedures in place collectively to mitigate a cyber-crisis on European level," said Enisa's executive director Professor Udo Helmbrecht. He added that the outcome of the exercise "will tell us where we stand and identify the next steps to take in order to keep improving."

- Europe hosts its biggest ever cyber security exercise, By Dave Neal, V3, 30 October 2014
- EU Cybersecurity Test Success, Network Security Agency Says, Dugie Standeford, Washingotn Internet Daily, 3 November 2014
- Cyber simulation, By staff, Professional Security, 30 October 2014

1.2 Spanish Coverage

- Brussels sheads light on infrastructures with its largest 'cybersecurity' exercise (Bruselas pone el foco en las infraestructuras en su mayor ejercicio de 'ciberseguridad'), By Staff, El Mundo, 31 October 2014

EL MUNDO

SECCIONES | Navegante | Gadgetoblog | Entre Bits&Chips | Player | Applicate | Jaque perpetuo | enrREDados

SEGURIDAD 'Cyber Europe 2014'

Bruselas pone el foco en las infraestructuras en su mayor ejercicio de 'ciberseguridad'

EL MUNDO | AGENCIAS › Madrid

Actualizado: 31/10/2014 **10:38 horas**

El mayor simulacro de 'ciberseguridad' hasta ahora en Europa reunió este jueves a más de 200 organizaciones y 400 expertos participantes. El ejercicio, llamado 'Cyber Europe 2014', ha girado en torno a **"una gran crisis que afecta a las infraestructuras críticas de información"**, informa la Comisión Europea.

De esta forma, este ejercicio conjunto se ha centrado sobre todo -y entre otras muchas amenazas- en **posibles ataques a infraestructuras críticas como las energéticas**, y la posibilidad de **ataques a las mismas redes de comunicaciones**.

El propio informe de ENISA sobre Panorama de Amenazas de 2013 ya **situaba las infraestructuras críticas en un lugar preferente**, "claves para la seguridad de la sociedad y las naciones". Tanto dichas infraestructuras como los principales componentes de **Sistemas de Control Industrial** (ICS por sus siglas en inglés) "están consideradas como **los mayores objetivos potenciales para grupos con gran capacidad de amenaza, sean terroristas o naciones**".

En declaraciones recogidas por The Register, **Steve Purser**, jefe de operaciones de Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), afirma que **"las mayores amenazas que estamos viendo realmente no son los ataques, sino los fallos de 'hardware' y 'software'"**.

"Sólo los esfuerzos conjuntos de este tipo ayudarán a asegurar la protección de la sociedad y la economía de hoy en día", declara por su parte la comisaria de Nuevas Tecnologías, **Neelie Kroes**, que insiste en que "la sofisticación y el volumen de ataques cibernéticos están aumentando todos los días ".

Noticias Relacionadas

Rosa Toue Inaugura la nueva flagship store de Bilbao

Lar España Real Estate adquiere el 59% de Puerta Marítima de Ondara

Leopoldo Abadía: 'todo indica' que se está 'en el buen camino' pero la salida de la crisis 'no será inmediata'

La economía de EEUU se desacelera pero crece más de lo previsto en el tercer trimestre

El informe del BBVA constata que 'la Comunidad crecerá más del 1% en 2014 y llegará al 2% en 2015'

Además

- 'Es una cuestión de tiempo que los 'ciberataques' tengan un impacto real en el mundo físico'
- Objetivo hacker: centrales energéticas
- Más temor por los sabotajes físicos que por los 'ciberataques'

De tiendas

"Hay cinco años no existía un procedimiento de cooperación entre los Estados miembros de la UE en caso de una cibercrisis" añade **Udo Helmbrecht**, director ejecutivo de ENISA. "El resultado del ejercicio de hoy nos dirá dónde nos encontramos e identificará los próximos pasos a dar para continuar mejorando".

La ENISA, que publicará un informe sobre este ejercicio, afirma que **los ataques cibernéticos en Internet en todo el mundo aumentaron en 2013 cerca de una cuarta parte y el número de violaciones de datos creció un 61% respecto de 2012**. Cada uno de los ocho violaciónes principales resultaron en la pérdida de decenas de datos.

'Cyber Europe' es un ejercicio bianual de ciberseguridad a gran escala. ENISA lo organiza cada dos años y este año cuenta con la participación de **29 países (26 de la UE y 3 de la AELC)**, además de instituciones de la UE. Hay tres fases: una **'técnica'**, finalizada en abril, que analiza las amenazas; otra **'táctico-operativa'**, dedicada a las acciones concretas para afrontar las diversas crisis -alertas, evaluación de la crisis, coordinación, intercambio de información y toma de decisiones- y una tercera **'estratégica'**, "que examina la toma de decisiones, el impacto político y los asuntos públicos".

- The most important cybersecurity exercise carried out in Europe (El ejercicio de seguridad cibernética más importante hecho en Europa), By Staff, La Vanguardia, 30 October 2014
- The largest ever test for cyber security organized in Europe, Cyber Europe 2014 (La ciberseguridad, a examen en el mayor ejercicio celebrado en Europa, Cyber Europa 2014), By Staff, EFE, 30 October 2014
- The EU carries out huge training exercises to counter possible cyber attacks (La UE lleva a cabo grandiosos entrenamientos para enfrentar un possible ciberataque), By Staff, RIA Novosti, 30 October 2014
- Important cyber security exercise in Europe (Importante ejercicio de ciberseguridad en Europe), By Staff, 30 October 2014
- Importante ejercicio de ciberseguridad en Europa, (Important cybersecurity exercise in Europe) By Staff, El Economista, 30 October 2014

elEconomista.es | Global
Jueves, 30 de Octubre de 2014 Actualizado a las 16:01
La Sareb adjudica a Solvia la gestión

Portada | Mercados y Cotizaciones | Empresas | Economía | Tecnología | Vivienda | Opinió

Actualidad | EcoDiario | GLOBAL | ESPAÑA | DEPORTES | MEDIO AMBIENTE | CULTURA | Program

Importante ejercicio de ciberseguridad en Europa

Twittear 0 Entrar g+1 0 Share

AFP | 30/10/2014 - 16:01

Puntúa la noticia : 1 10 Nota de los usuarios: - (0 votos)

Más de 200 organizaciones y 400 expertos de ciberseguridad de 29 países europeos participaban este jueves en el más vasto ejercicio de ciberseguridad que se ha organizado en Europa, indicó la Comisión Europea.

El ejercicio, bautizado "Cyber Europe 2014" simula "una crisis a gran escala que afecte infraestructuras de información esenciales", señala en un comunicado.

El escenario contempla más de 2.000 "ciberincidentes", desde ataques por denegación de servicio -con los que se bloquea una página internet con una avalancha de solicitudes-, "la exfiltración de informaciones sensibles, ataques contra infraestructuras esenciales tales como la red de energía o de telecomunicaciones", entre otros ejemplos citados.

El comunicado precisa que el ejercicio implica a varios centros de toda Europa.

"Sólo los esfuerzos comunes de este tipo contribuirán a mantener la protección de la sociedad y de la economía", señaló la comisaria a cargo de Nuevas Tecnologías, Neelie Kroes.

"Hace cinco años no existía ningún procedimiento de cooperación entre los Estados miembros de la UE en caso de cibercrisis", dijo por su parte Udo Helmbrecht, director de la agencia europea a cargo de la seguridad de las redes de información (Enisa).

Enisa publicará un informe con los resultados del ejercicio. Según la agencia, los ciberataques en internet a escala mundial aumentaron en 2013 de casi un cuarto.

- Europe carries out a grand scale information security exercise (Europa realiza ejercicio a gran escala de seguridad informática), By Staff, Panama On, 30 October 2014
- "Cyber Europe 2014" the most extensive cyber security exercise in Europe ("Cyber Europe 2014", el ejercicio de ciberseguridad más extenso de Europa), By Camilo Bravo, 24horas, 30 October 2014
- Mega exercise in the European Union against cyber attacks (Mega ejercicio en Unión Europea contra ataques cibernéticos), By Staff, La Cronica, 30 October 2014
- Largest cyber security exercise in Europe to date takes place today (Se realiza hoy el mayor ejercicio de ciberseguridad de Europa hasta la fecha), By Staff, ICNDiario, 30 October 2014
- EU carries out mega exercise against cyber attacks (UE realiza mega ejercicio contra ciberataques), By Staff, 30 October 2014
- The European Union carries out mega simulation against cyber attacks (Unión Europea realiza mega simulacro contra ataque cibernéticos), By Staff, Poblanerías, 30 October 2014

1.3 French Coverage

- The EU holds its largest cyber security exercise ever conducte to date (L'UE organise son plus grand exercice de cybersécurité jamais réalisé jusqu'ic), By Staff, People Daily, 31 October 2014

- Large cybersecurity exercise in Europe (Vaste exercice de cybersécurité en Europe), By Staff, AFP, 30 October 2014 (*full text below*)
    - Bilan
- Largest ever cybersecurity exercise in Europe taking place today (Le plus grand exercice de cyber sécurité en Europe a lieu aujourd'hui), By Marc Jacob, Global Security Mag, 30 October 2014
- And if a cyber attack caused the ruin of a nation? (et si une cyberattaque causait la perte d'une nation?), By Staff, IT espresso, 30 October 2014
- Luxembourgish particiation in the second exercise phase of "Cyber Europe 2014" (Participation luxembourgeoise à la seconde phase de l'exercice "Cyber Europe 2014"), By Staff, Gouvernment.lu, 30 October 2014
- Luxembourg participates in the "Cyber Europe 2014" exercise (Le Luxembourg participe à l'exercice «Cyber Europe 2014») By Jessica Cencetti, ITnation.lu, 30 October 2014
- Could a cyber attack cripple a nation by 2025 ? (Une cyberattaque peut-elle paralyser une nation d'ici 2025 ?), By Ariane Beky, Silicon, 30 October 2014
- Large cybersecurity exercise (Vaste exercice de cybersécurité), By Staff, Le Devoir, 30 October 2014

EUROPE

Vaste exercice de cybersécurité

30 octobre 2014 20h12 | La Presse canadienne | Europe

Photo: iStock

Bruxelles — Plus de 400 experts en cybersécurité participaient jeudi au plus grand exercice de simulation ayant jamais eu lieu en Europe, a indiqué la Commission européenne.

L'exercice baptisé « Cyber Europe 2014 » simulait *« une crise de grande ampleur affectant des infrastructures d'information essentielles »*.

Plus de 2000 incidents étaient traités, indique la Commission, citant notamment des attaques contre des services en ligne, des rapports des services de renseignement et des reportages des médias sur des cas de cyberattaque, ainsi que des « défacements » de sites Web (attaques modifiant leur aspect), des exfiltrations d'informations sensibles et des attaques contre des réseaux d'énergie ou de télécoms.

1.4 Italian Coverage

- Cyber Europe: the largest European cybersecurity exercise takes place today (Cyber Europe: oggi la più grande esercitazione europea sulla sicurezza informática), By Staff, Help Consumatori, 30 October 2014
- Cybersecurity: the largest-ever exercise in Europe (Sicurezza informatica, al via la più grande esercitazione di sempre in Europa), By Staff, il Velino, 30 October 2014

- #CyberEurope2014: CE, cybersecurity exercise (#Cybereurope2014: CE, esercitazione sulla sicurezza informatica), By Staff, Agenzia Giornalistica Globalpress, 30 October 2014

1.5 German Coverage

- Today: the largest cybersecurity exercise in Europe so far (Heute: Bisher größte Übung zur Cybersicherheit in Europa), By Staff, 02elf Düsseldorfer Abendblatt, 31 October 2014
- Cyber Europe 2014: Large-scale exercise on cybersecurity in Europe (Cyber Europe 2014: Großangelegte Übung zur Cybersicherheit in Europa), By Rudolf Felser, Computerwelt, 30 October 2014

30.10.2014 pi/Rudolf Felser

Cyber Europe 2014: Großangelegte Übung zur Cybersicherheit in Europa

Mehr als 200 Organisationen und 400 Cybersicherheitsexperten aus 29 europäischen Ländern testen heute in einer ganztägigen Simulation, wie gut sie auf eventuelle Cyberangriffe vorbereitet sind.

© Data Nmedia - Fotolia.com

Organisiert wird die Übung von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA). Im Rahmen eines realitätsnahen, großangelegten Cybersicherheitsszenarios – Cyber Europe 2014 – stellen Fachleute aus dem öffentlichen und dem privaten Sektor, darunter Netzsicherheitsbehörden, nationale IT-Notfallteams, Ministerien, Telekommunikations- und Energieunternehmen, Finanzinstitute und Internetdienstleister ihre Verfahren und Fähigkeiten zur Abwehr von Gefahren im Netz auf den Prüfstand. Es wird eine Krise von großem Ausmaß im Zusammenhang mit kritischen Informationsinfrastrukturen simuliert. Fachleute der ENISA verfassen anschließend einen Bericht zu den wichtigsten aus der Übung gewonnenen Erkenntnissen.

Cyber Europe 2014 ist die größte und komplexeste Übung dieser Art, die bisher in Europa stattgefunden hat. Mehr als 2000 verschiedene Cybervorfälle werden durchgespielt, u. a. Überlastungsangriffe auf Online-Dienste, Erkenntnisse und Medienberichte über Cyberangriffe, Website-Defacement (Angriffe, bei denen das Erscheinungsbild von Websites widerrechtlich verändert wird), Ausspionieren sensibler Informationen und Angriffe auf kritische Infrastrukturen wie Energie- oder Telekommunikationsnetze. Außerdem werden die Zusammenarbeit in der EU sowie Eskalationsverfahren getestet. Es handelt sich hierbei um eine auf mehrere Zentren in ganz Europa verteilte Übung, die von einem zentralen Kontrollzentrum koordiniert wird.

Der Direktor der ENISA, Udo Helmbrecht, erklärte: "Vor fünf Jahren gab es noch keine Verfahren zur Unterstützung der Zusammenarbeit zwischen den EU-Mitgliedstaaten im Falle einer Cyberkrise. Heute stehen diese gemeinsamen Verfahren und helfen bei der Bewältigung solcher Krisen in Europa. Das Ergebnis der heutigen Übung wird zeigen, wo wir stehen und welche Schritte als nächstes unternommen werden müssen, um die Verfahren weiter zu verbessern."

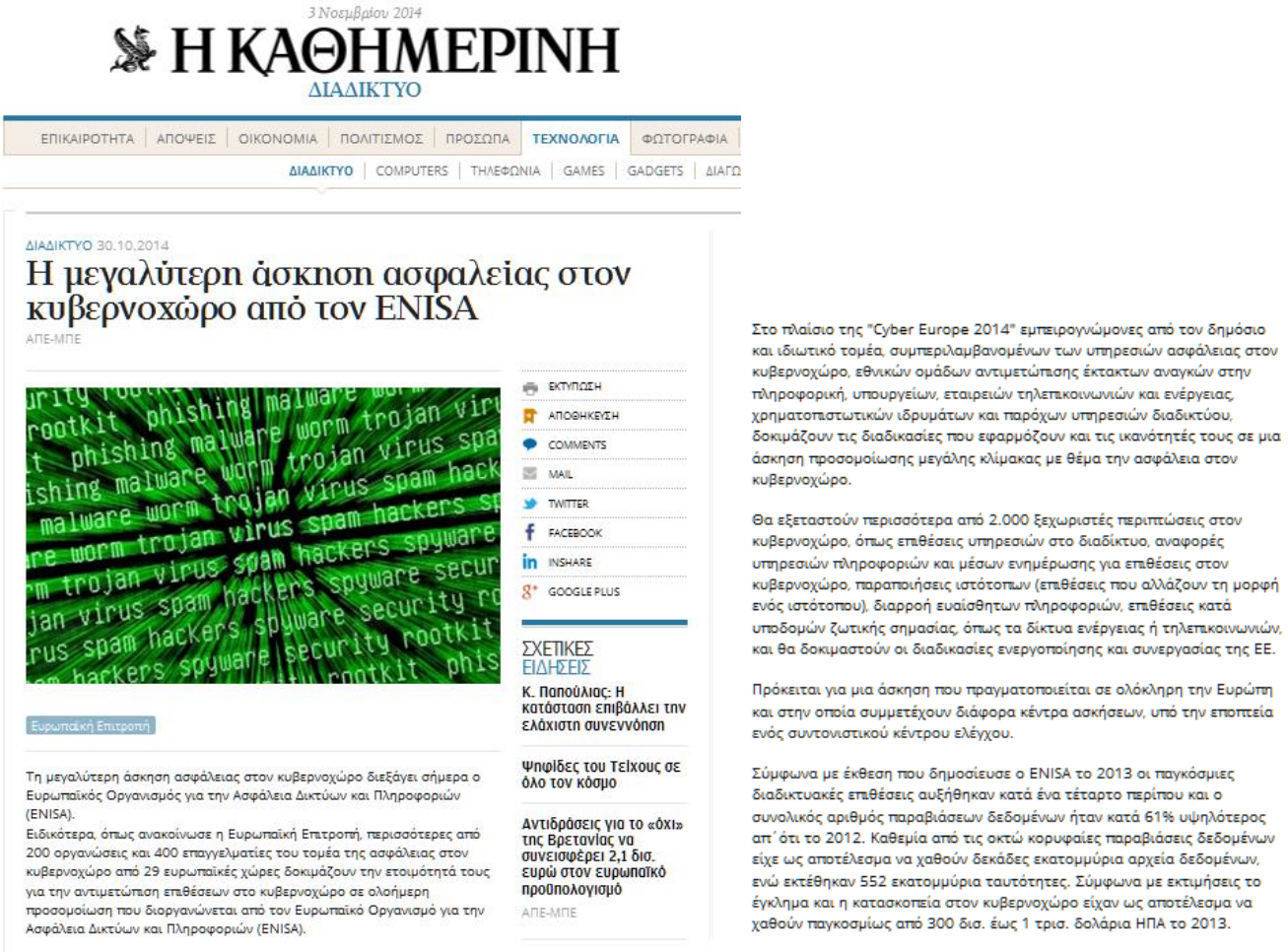
Im Rahmen der Übung werden unter anderem Verfahren für den Austausch operativer Informationen über Cyberkrisen in Europa erprobt, die nationalen Fähigkeiten zur Bewältigung von Cyberkrisen gestärkt und die Auswirkungen eines multiplen und parallelen Informationsaustauschs zwischen dem öffentlichen und dem privaten Sektor und innerhalb des Privatsektors auf nationaler und internationaler Ebene untersucht. Bei der Übung werden zudem die operativen Standardverfahren der EU (EU-SOP) getestet. Dabei handelt es sich um Leitlinien für den Austausch von operativen Informationen über Cyberkrisen.

Die Übung besteht aus drei über das Jahr verteilten Phasen: der technischen Phase (abgeschlossen im April), die die Aspekte Erkennung und Untersuchung von Cybervorfällen, Eindämmung und Informationsaustausch umfasst; der operativen/taktischen Phase (heute und Anfang 2015), in der Warnung, Krisenbewertung, Zusammenarbeit, Koordinierung, taktische Analyse, Beratung und Informationsaustausch auf operativer Ebene im Mittelpunkt stehen, und der strategischen Phase, in der Entscheidungsprozesse, politische Auswirkungen und Öffentlichkeitsaspekte behandelt werden. Während der Übung werden kritische Informationsinfrastrukturen, -systeme oder -dienste nicht beeinträchtigt. (pi)

- Cyber-attacks: Europe under virtual attack (Cyber-Attacken: Europa unter virtuellem Beschuss), By Jeremy Fleming, 30 October 2014
- European experts test network security in the largest cyber exercise to date (Europäische Experten testen in bisher größtem Cybermanöver Netzsicherheit), By Stefan Krempl, Heise Newsticker, 30 October 2014
  Cyber Europe 2014: 29 European countries try to act against cyber attacks (Cyber Europe 2014: 29 europäische Länder testen Handlungsfähigkeit gegen Cyberattacken) By Staff, Heise, IX, 30 October 2014
- The largest cybersecurity exercise in Europe so far (Bisher größte Übung zur Cyber-Sicherheit in Europa), By Staff, All About SECURITY, 30 October 2014

1.6 Greek Coverage

- The largest cyber security exercise by ENISA (Η μεγαλύτερη άσκηση ασφαλείας στον κυβερνοχώρο από τον ENISA), By Staff, ANA-MPA, 30 October 2014
  Syndicated by:
  - Kathimerini



3 Νοεμβρίου 2014

Η ΚΑΘΗΜΕΡΙΝΗ

ΔΙΑΔΙΚΤΥΟ

ΕΠΙΚΑΙΡΟΤΗΤΑ | ΑΠΟΨΕΙΣ | ΟΙΚΟΝΟΜΙΑ | ΠΟΛΙΤΙΣΜΟΣ | ΠΡΟΣΩΠΑ | ΤΕΧΝΟΛΟΓΙΑ | ΦΩΤΟΓΡΑΦΙΑ

ΔΙΑΔΙΚΤΥΟ | COMPUTERS | ΤΗΛΕΦΩΝΙΑ | GAMES | GADGETS | ΔΙΑΓΩ

ΔΙΑΔΙΚΤΥΟ 30.10.2014

Η μεγαλύτερη άσκηση ασφαλείας στον κυβερνοχώρο από τον ENISA

ΑΠΕ-ΜΠΕ

ΕΚΤΥΠΩΣΗ
ΑΠΟΘΗΚΕΥΣΗ
COMMENTS
MAIL
TWITTER
FACEBOOK
INSHARE
GOOGLE PLUS

ΣΧΕΤΙΚΕΣ ΕΙΔΗΣΕΙΣ

Κ. Παπούλιας: Η κατάσταση επιβάλλει την ελάχιστη συνεννόηση

Ψηφίδες του Τείχους σε όλο τον κόσμο

Αντιδράσεις για το «όχι» της Βρετανίας να συνεισφέρει 2,1 δισ. ευρώ στον ευρωπαϊκό προϋπολογισμό

ΑΠΕ-ΜΠΕ

Ευρωπαϊκή Επιτροπή

Τη μεγαλύτερη άσκηση ασφαλείας στον κυβερνοχώρο διεξάγει σήμερα ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).
Ειδικότερα, όπως ανακοίνωσε η Ευρωπαϊκή Επιτροπή, περισσότερες από 200 οργανώσεις και 400 επαγγελματίες του τομέα της ασφάλειας στον κυβερνοχώρο από 29 ευρωπαϊκές χώρες δοκιμάζουν την ετοιμότητά τους για την αντιμετώπιση επιθέσεων στο κυβερνοχώρο σε ολοήμερη προσομοίωση που διοργανώνεται από τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).

Στο πλαίσιο της "Cyber Europe 2014" εμπειρογνώμονες από τον δημόσιο και ιδιωτικό τομέα, συμπεριλαμβανομένων των υπηρεσιών ασφάλειας στον κυβερνοχώρο, εθνικών ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική, υπουργείων, εταιρειών τηλεπικοινωνιών και ενέργειας, χρηματοπιστωτικών ιδρυμάτων και παρόχων υπηρεσιών διαδικτύου, δοκιμάζουν τις διαδικασίες που εφαρμόζουν και τις ικανότητές τους σε μια άσκηση προσομοίωσης μεγάλης κλίμακας με θέμα την ασφάλεια στον κυβερνοχώρο.

Θα εξεταστούν περισσότερα από 2.000 ξεχωριστές περιπτώσεις στον κυβερνοχώρο, όπως επιθέσεις υπηρεσιών στο διαδίκτυο, αναφορές υπηρεσιών πληροφοριών και μέσων ενημέρωσης για επιθέσεις στον κυβερνοχώρο, παραποιήσεις ιστότοπων (επιθέσεις που αλλάζουν τη μορφή ενός ιστότοπου), διαρροή ευαίσθητων πληροφοριών, επιθέσεις κατά υποδομών ζωτικής σημασίας, όπως τα δίκτυα ενέργειας ή τηλεπικοινωνιών, και θα δοκιμαστούν οι διαδικασίες ενεργοποίησης και συνεργασίας της ΕΕ.

Πρόκειται για μια άσκηση που πραγματοποιείται σε ολόκληρη την Ευρώπη και στην οποία συμμετέχουν διάφορα κέντρα ασκήσεων, υπό την επιστασία ενός συντονιστικού κέντρου ελέγχου.

Σύμφωνα με έκθεση που δημοσίευσε ο ENISA το 2013 οι παγκόσμιες διαδικτυακές επιθέσεις αυξήθηκαν κατά ένα τέταρτο περίπου και ο συνολικός αριθμός παραβιάσεων δεδομένων ήταν κατά 61% υψηλότερος απ΄ότι το 2012. Καθεμία από τις οκτώ κορυφαίες παραβιάσεις δεδομένων είχε ως αποτέλεσμα να χαθούν δεκάδες εκατομμύρια αρχεία δεδομένων, ενώ εκτέθηκαν 552 εκατομμύρια ταυτότητες. Σύμφωνα με εκτιμήσεις το έγκλημα και η κατασκοπεία στον κυβερνοχώρο είχαν ως αποτέλεσμα να χαθούν παγκοσμίως από 300 δισ. έως 1 τρισ. δολάρια ΗΠΑ το 2013.

- ENISA: Preparedness exercise for the security of Internet (ENISA: Ασκηση ετοιμότητας για την ασφάλεια του Internet), Ο Φιλελεύθερος, 31 October 2014
- EU: cybersecurity exercise (ΕΕ: Άσκηση ασφάλειας στον κυβερνοχώρο0), By Staff, Real.gr, 31 October 2014
- Cyber Europe 2014: Pan-European exercise for cybersecurity (Cyber Europe 2014: Πανευρωπαϊκή άσκηση για την ασφάλεια στον κυβερνοχώρο), By Staff, euronews, 30 October 2014
- The largest European security “web-exercise” in Athens (Η μεγαλύτερη ευρωπαϊκή "web-άσκηση" ασφαλείας στην Αθήνα), By Staff, MEGA TV, 30 October 2014
- The largest cybersecurity exercise in Europe so far (Πραγματοποιείται η μεγαλύτερη μέχρι τώρα άσκηση ασφάλειας στον κυβερνοχώρο στην Ευρώπη), By Staff, Prisma News, 30 October 2014
- The biggest cyber security exercise is coordinated from Greece (Η μεγαλύτερη άσκηση στην ΕΕ για την κυβερνο-ασφάλεια, με συντονισμό από την Ελλάδα) By Staff, Nerit, 30 October 2014
- The largest cybersecurity exercise in Europe (Η μεγαλύτερη άσκηση σχετικά με την ασφάλεια στον κυβερνοχώρο στην Ευρώπη), By Staff, Diorismos, 30 October 2014
- EU preparedness exercise for the security of the Internet (Ασκηση ετοιμότητας για την ασφάλεια του Internet θα κάνει η Ε.Ε.), By Staff, tovima, 30 October 2014

- Cyber Europe 2014: Πανευρωπαϊκή άσκηση για την ασφάλεια στον κυβερνοχώρο (Cyber Europe 2014, Pan-European Exercise for cyber security), By Staff, gr.euronews, 30 October 2014

1.7 Portuguese Coverage

- Europe holds its largest and most complex cybersecurity exercise (Europa realiza o seu maior e mais complexo exercício de cibersegurança), By Staff, Público, 30 October 2014

Europa realiza o seu maior e mais complexo exercício de cibersegurança

PÚBLICO 30/10/2014 - 13:48

Portugal e 28 países vão testar a capacidade de resposta a ataques informáticos.

KACPER PEMPEL/REUTERS

Iniciar Tweetar 0 +1 6

TÓPICOS

Europa
União Europeia
Crime
Segurança interna
Cibersegurança
Comissão Europeia
Internet

MAIS

- Nato, UE e governo ucraniano foram alvo de ataque informático russo
- Yahoo! foi alvo de ataques a partir da Roménia
- Centro de

Durante toda esta quinta-feira, 29 países europeus, incluindo Portugal, estão a realizar em conjunto um exercício de cibersegurança para testar o grau de preparação de cada Estado para combater ataques informáticos de grande escala. Mais de 200 organizações e 400 profissionais da área do sector público e privado integram o exercício, durante o qual haverá uma simulação de vários ciberataques e será analisada a capacidade de resposta de cada país e a nível europeu.

Esta é a terceira vez que se realiza o Cyber Europe 2014, depois das edições de 2010 e 2012. Este ano, o exercício, que é organizado pela Agência Europeia para a Segurança das Redes e Informação (ENISA), é mais vasto e complexo que nos anos anteriores e engloba 26 estados-membros da União Europeia e três países da Associação Europeia de Comércio Livre (EFTA, na sigla em inglês).

Em cada estado vão estar envolvidas, caso existam, agências de cibersegurança, equipas nacionais de resposta a emergências informáticas, ministérios, empresas de telecomunicações, empresas do sector da energia instituições financeiras e prestadores de serviços de Internet .

- Today Europe tests response to a cyber attack (Europa testa hoje resposta a ciberataque), By Staff, Jornal SOL, 30 October 2014
- Europe is now the target of a cyberattack (Europa será hoje alvo de um ciberataque), By Staff, Diário de Notícias, 30 October 2014 By Staff, Jornal SOL, 30 October 2014
- Europa testa resposta a ciberataque (Europe tests cyber attack response) By Staff, ionline.pt, 30 October 2014
- Europe is conducting an important cybersecurity exercise (Europa faz importante exercício de cibersegurança), By Staff, NE10, 30 October 2014
- O maior exercício de cibersegurança na Europa realiza-se hoje (The largest cybersecurity exercise in Europe is being held today), By staff, Diario Digital, 30 October 2014
- Bruxelas Europa testa hoje resposta a ciberataque (Brussels, Europe tests today response against cyber attacks) By staff, Notícias ao Minuto, 30 October 2014

1.8 Other Languages

- Grootste simulatie van cyberaanvallen in Europa ooit (Biggest ever simulation of cyber attacks in Europe) NL, By staff, Security.nl, 30 October 2014
- Norisinās līdz šim Eiropā lielākās kiberdrošības mācības (Europe's largest ever cyber security training taking place)LT, By staff, tvnet.lv, 30 October 2014
- Europa houdt grootste cyberoefening ooit, (Europe's biggest ever cyber exercise) NL, By staff, hln.be, 30 October 2014
- ЕС провежда най-голямото учение по киберсигурност (EU holds the largest study on cyber security) by Staff, dnevnik.bg, 30 October 2014

1.9 Full Text of Articles

"Working together helps build confidence"
By Nathalie Steiwer
Europolitics
31 October 2014

Interview with Udo Helmbrecht, executive director, ENISA

The third major pan-European exercise in cyber security was organised on 30 October by the European Union Agency for Network and Information Security (ENISA). The Executive Director of the agency, Udo Helmbrecht, draws conclusions from these experiences in view of the legislative negotiations underway on the network security directive (NIS).

What is the purpose of the Cyber Europe 2014 exercise, bringing together 400 public and private experts from Europe?

We are testing our standard response procedures to cyber attacks at the technical and political level: how we respond to incidents, how we document them, how to obtain aid. The results will help us to identify the next steps and what needs to be improved. Since the first exercise in 2010, we have been proceeding in stages. Beginning with the governmental level, we realised that we did not even have a list of telephone contacts in all member states. In some countries, interior ministers are responsible for cyber security, while elsewhere it is the economy or defence minsters. We now have these governmental contacts but it is not sufficient: 80% of infrastructure in Europe falls under the private sector. We have therefore brought together one hundred or so participants from the financial and banking sector in particular.

What conclusions can you draw from these exercises?

The construction of a community and of capacity are two important factors. We learn which profiles we need in the ministries, what the technical requirements are and the decisions necessary on a political level. As in the fight against criminality within Europol, some member states have a long history of cooperation, while others do not. We need all member states to reach the same level of capacity.

If such cooperation already exists, what will be the purpose of the NIS directive?

Ideally, we should have an ecosystem which operates autonomously, but in certain areas this is not the case. The directive makes it possible to generalise procedures by allowing member states a margin of manoeuvre for their implementation. Practically all member states have adopted a national strategy for cyber security. They are

published on our website. The missing three or four strategies should be ready at the beginning of 2015. The NIS directive would push all member states to effectively implement certain things.

Why impose the notification of IT incidents?

Industry states that notifications are a burden to manage from an administrative point of view, but enterprises such as governments need data to make the right decisions. In the framework of the telecoms regulation, which already imposes notifications in this sector, we learnt, for example, that the challenges are not so much viruses, but having energy rescue facilities.

At the Council, member states are refusing to be obliged to exchange confidential information. Have the exercises not reinforced trust? The exercises make it possible to have a common understanding of threats: from the classical phishing to the stuxnet virus targeting infrastructures. Working together then helps to build personal associations so that people can trust one another and begin to share confidential information on national problems or best practice.

The problem is that there is a slight difference between the confidential information that you provide to somebody you trust and that which is included in an official document.

In light of this experience, which businesses should be obliged to provide notifications?

The current telecoms regulation already includes internet access providers and progress has been made with the banking sector on a voluntary basis. The problem now is that we are talking about a highly competitive sector: we must be sure that competitors will not use the incidents declared by others as a commercial argument. Being transparent must not be a competitive disadvantage. We must above all identify what falls under the responsibility of the government, what the critical infrastructures are: energy, water, cash points... The problem is that some of these structures are private, while others are public. We therefore need a good definition of the types of structures concerned. The list of businesses concretely involved will automatically follow on from this.

Vaste exercice de cybersécurité en Europe
By Staff
Agence France Presse
30 October 2014

Plus de 400 experts en cybersécurité participaient jeudi au plus grand exercice de simulation ayant jamais eu lieu en Europe, a indiqué la Commission européenne.
L'exercice baptisé "Cyber Europe 2014" simulait "une crise de grande ampleur affectant des infrastructures d'information essentielles".

Plus de 2.000 incidents étaient traités, indique la Commission, citant notamment des attaques contre des services en ligne, des rapports des services de renseignement et des reportages des médias sur des cas de cyberattaque, ainsi que des "défacements" de sites web (attaques modifiant leur aspect), des exfiltrations d'informations sensibles et des attaques contre des réseaux d'énergie ou de télécoms.

Cet exercice mobilisait plus de 200 organisations et 400 professionnels de 29 pays européens. Il impliquait plusieurs centres d'exercice dans toute l'Europe, dont la coordination est assurée par un centre de contrôle central, selon l'exécutif européen.
"Seuls des efforts communs de ce type contribueront au maintien de la protection de la société et de l'économie d'aujourd'hui", a souligné la commissaire en charge des Nouvelles technologies, Neelie Kroes, insistant sur le fait que "la sophistication et le volume des cyberattaques augmentent tous les jours".

"Il y a cinq ans, il n'existait aucune procédure de coopération entre les États membres de l'Union en cas de cybercrise", a renchéri Udo Helmbrecht,le directeur général de l'Agence européenne chargée de la sécurité des réseaux d'information (Enisa).

"Aujourd'hui, les procédures permettant d'atténuer une cybercrise au niveau européen sont en place collectivement. Le résultat de l'exercice nous dira où nous en sommes et permettra d'identifier les prochaines mesures à prendre en vue de continuer à améliorer la situation", a-t-il estimé.

L'Enisa publiera ensuite un rapport sur cet exercice. Selon l'agence, les cyberattaques sur internet à l'échelle mondiale ont augmenté en 2013 de près d'un quart et le nombre total de violations de données était supérieur de 61% à celui de 2012. Chacune des huit principales violations a abouti à la perte de dizaines de données.

La Commission a proposé début 2013 un plan de lutte qui obligera les Etats à adopter une stratégie en matière de sécurité des réseaux d'information et à désigner des autorités nationales compétentes.

BIGGEST THREAT to Europe's cybersecurity? Hint: not hackers - Largest EVER Europe-wide cybersecurity exercise, The Register

By Jennifer Baker and John Leyden
30 Oct 2014

Forget cyber-espionage, cyber-warfare and cyber-terrorism. The biggest threat to Europe's infrastructure cybersecurity are power outages and poor communication.

On Thursday, ENISA (European Network and Information Security Agency) held its biggest ever cybersecurity exercise involving more than 200 organisations and 400 cyber-security professionals from 29 European countries.

The bi-annual* event simulates a lifelike attack, modelled on real events, to test the reaction of national Computer Emergency Response Teams (CERTS), government ministries, telco companies, energy companies, financial institutions and internet service providers.

But Steve Purser, Head of Operations at ENISA explained: "The biggest threats we really see are not attacks, but hardware and software failures."

#CyberEurope2014 will simulate more than 2,000 separate cyber-incidents, including denial of service attacks, website defacements, exfiltration of sensitive information and attacks on critical infrastructure.

Purser says he's confident that they are testing the right things. "I speak at a lot of events and there are a lot of glib comments from people saying we need to share more data. But actually we need to share LESS data. We live in an age of data pollution and we need to discuss the right things at the right level."

This would appear to include a standard array of attacks that systems need to be tested against but nothing particularly tricky such as exploitation of unpatched vulnerabilities, custom malware, data contamination or social engineering.

The distributed exercise, involving several exercise centres across Europe working with a central exercise control centre, is designed to test EU cooperation and escalation procedures. The exercise will also test out the EU-Standard Operational Procedures, a set of guidelines to share operational information on cyber crisis.

In the case of the Spanish military, at least, the exercise involves military personnel in camouflage uniforms (¿Por qué?) crowded together around laptops and wide screens in a crowded room on the outskirts of Madrid. A picture by OneMagazine illustrates the claustrophobic scene, seemingly devoid of tapas, cafe or other Spanish essentials.

Last year global web-based attacks increased by almost a quarter and the total number of data breaches was 61 per cent higher than 2012 according to Symantec's Intelligence Report.

Each of the eight top data breaches resulted in the loss of tens of millions of data records while 552 million identities were exposed. Meanwhile, ENISA's Threat Landscape report says that threat agents have increased the sophistication of their attacks and their tools and multiple countries have developed capabilities that can be used to infiltrate all kinds of targets, governmental and private.

The proposed EU Network and Information Security Directive, (aka the Cybersecurity Directive) aims to address these problems. The draft law is currently being discussed by national representatives, the European Parliament and the European Commission.

Some elements of the original law have already been substantially watered down. Originally "key internet enablers" faced mandatory security breach and incident notification requirements, but this was changed by the European Parliament and the provision now applies only to "market operators who provide critical infrastructure".

Who and what these market operators are is vaguely worded and a cause for dispute between member states at the negotiating table.

"Member states deal with critical infrastructure in different ways - some are asset based, some process based and the challenge is to put those together. It's a complex situation," said Purser adding that events like CyberEurope2014 help to identify weaknesses.

He believes the proposed directive is a step in the right direction: national governments would still be required to appoint a competent central authority and develop a national cybersecurity strategy. These national authorities would be required to liaise with ENISA and an EU-wide "Cooperation Network".

Professor Udo Helmbrecht, executive director of ENISA, commented: "Five years ago there were no procedures to drive cooperation during a cyber-crisis between EU Member States. Today we have the procedures in place collectively to mitigate a cyber-crisis on European level. The outcome of today's exercise will tell us where we stand and identify the next steps to take in order to keep improving."

However there is considerable resistance from some national representatives to mandatory sharing of information between countries as envisaged in the current draft law. Some countries fear giving away too much information to subjecting companies to "reputational damage".

Based on previous CyberEurope events, Purser thinks that those involved are getting better at sharing information, and he was keen to stress that “we are not talking about industrial espionage, which I think is a false debate. [ENISA] is not interested in handling national security information. But exercises like this provide valuable bottom-up knowledge behind the policy.”

ENISA will produce a report on its findings from Thursday’s exercise by the end of the year, while the next discussion between national representatives on the cybersecurity directive will take place on November 27. Bootnote

*Cyber Europe actually takes place in three phases throughout the year: technical – which involves the incident detection, investigation, mitigation and information exchanges (completed in April); operational/tactical – dealing with alerting, crisis assessment, cooperation, coordination, tactical analysis, advice and information exchanges at operational level (today and early 2015); and strategic, which examines decision making, political impact and public affairs. Thursday's activities form the main part of the whole exercise.

ENISA promises that the exercise will not affect critical information infrastructures, systems, or services.