enisa
European Network and Information Security Agency

Cyber Europe 2012

Huvudsakliga resultat och rekommendationer

December 2012

Författarnas tack

Enisa vill tacka alla personer och organisationer som har bidragit till denna övning. Vårt tack går särskilt till övningsplanerare, nationella övervakare och moderatorer.

Om Enisa

Europeiska byrån för nät- och informationssäkerhet (Enisa) är ett expertiscentrum för nätverks- och informationssäkerhet för EU, dess medlemsstater, den privata sektorn och de europeiska medborgarna. Enisa arbetar tillsammans med dessa grupper för att ta fram råd och rekommendationer om god praxis för informationssäkerhet. Byrån hjälper också EU-medlemsstaterna i genomförandet av relevant lagstiftning och arbetar för att förbättra motståndskraften hos Europas kritiska informationsinfrastruktur och informationsnät. Enisas mål är att stärka den befintliga sakkunskapen i EU:s medlemsstater genom att stödja utvecklingen av gränsöverskridande expertgrupper som arbetar för att förbättra nät- och informationssäkerheten i EU. Mer information om Enisa och byråns arbete finns på www.enisa.europa.eu.

Följ oss på Facebook Twitter LinkedIn Youtube och RSS feeds

Enisas projektgrupp

Panagiotis Trimintzios, Enisa
Razvan Gavrila, Enisa
Maj Ritter Klejnstrup, Enisa

Kontaktuppgifter

Frågor om denna rapport eller andra allmänna frågor om programmet för stärkande av motståndskraften hos Europas kritiska informationsinfrastruktur och informationsnät kan skickas till följande adress: resilience at enisa.europa.eu

Innehåll

Om Cyber Europe 2012

Den 4 oktober 2012 deltog över 500 experter på it-säkerhetsområdet i Europa i Cyber Europe 2012, den andra Europatäckande it-övningen.

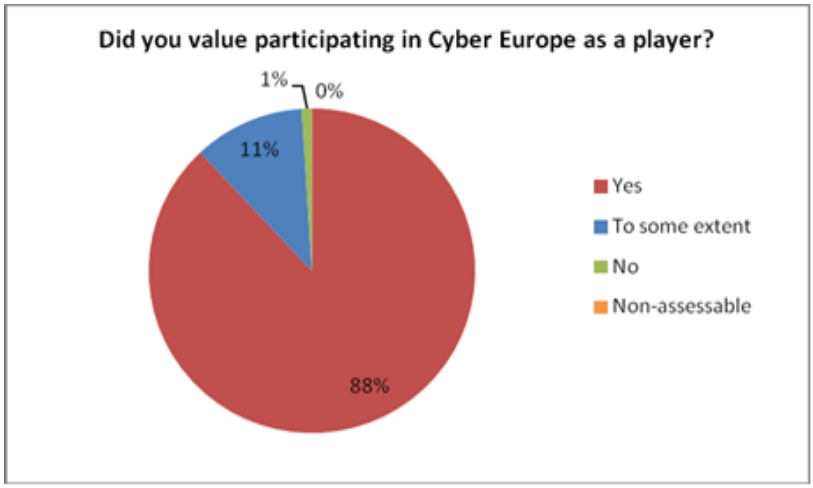
Övningen byggde på ett omfattande arbete på både nationell och europeisk nivå för att förbättra motståndskraften hos kritiska informationsinfrastrukturer. Därför var Cyber Europe 2012 en milstolpe i insatserna för att stärka samarbetet, beredskapen och insatserna vid it-kriser i Europa.

År 2009 offentliggjorde Europeiska kommissionen ett meddelande om skydd av kritisk informationsinfrastruktur: ”Skydd mot storskaliga it-attacker och avbrott: förbättrad beredskap, säkerhet och motståndskraft i Europa” (KOM/2009/149). Meddelandet gav upphov till den första Europatäckande cyberövningen, som genomfördes den 4 november 2010. Kommissionen går vidare med sin digitala agenda för Europa (2010) och sitt meddelande från 2011: ”Resultat och kommande åtgärder: vägen mot global it-säkerhet” (KOM/2011/163). Som ett resultat av dessa insatser utökades Cyber Europe 2012 i räckvidd, omfattning och komplexitet.

Cyber Europe 2012 hade följande tre mål:

1. Testa effektiviteten och skalbarheten hos mekanismer, förfaranden och informationsflöden för samarbete mellan offentliga myndigheter i Europa.
2. Undersöka samarbetet mellan offentliga och privata aktörer i Europa.
3. Kartlägga luckor och problem när det gäller en effektivare hantering av storskaliga it-säkerhetsincidenter i Europa.

Tjugonio EU-medlemsstater (Europeiska unionen) och Eftaländer (Europeiska frihandelssammanslutningen) deltog i övningen. Av dessa deltog 25 medlemsländer aktivt i övningen, medan de övriga fyra länderna deltog som observatörer. Dessutom deltog flera EU-institutioner. Sammanlagt deltog 339 organisationer i övningen, med totalt 571 individuella aktörer. Som uppföljning av en huvudrekommendation från Cyber Europe 2010 deltog aktörer från den privata sektorn i övningen. Samarbetet mellan offentliga och privata aktörer genomfördes på nationell nivå, medan de offentliga myndigheterna även samarbetade över gränserna. De flesta aktörer (88 procent) såg positivt på övningen (se Figur 1).



Figur 1: Nivån på aktörernas tillfredsställelse

Uppskattade du att delta som aktör i Cyber Europe?

- Ja,
- I viss utsträckning,
- Nej,
- Vet ej

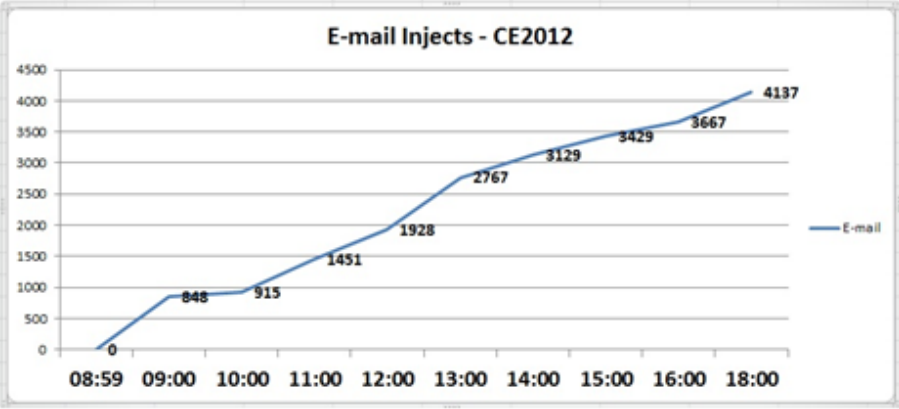
Planeringsprocessen

Cyber Europe 2012 anordnades av Europeiska byrån för nät- och informationssäkerhet (Enisa) och stöddes tekniskt av Europeiska kommissionens gemensamma forskningscenter (JRC). Företrädare från samtliga 25 deltagande länder och EU-institutioner deltog i planeringen av övningen. Planeringsprocessen organiserades kring flera seminarier.

Scenariot

Övningsscenariot handlade om storskaliga it-säkerhetsincidenter i Europa, som påverkade alla deltagande länder. Fiktiva motståndare slog ihop sig i en massiv it-attack mot Europa, främst genom DDoS-attacker (Distributed denials of service) mot offentliga elektroniska tjänster. De drabbade tjänsterna var e-förvaltningstjänster och finansinstitut (e-banker etc.).

It-säkerhetsincidenterna utmanade deltagarna från den offentliga och den privata sektorn och utlöste ett behov av gränsöverskridande samarbete. Aktörerna fick information om scenariot (”injektioner”) via e-post, och skulle samarbeta genom att tillämpa standardförfaranden och standardstrukturer för att bedöma situationen och enas om en gemensam handlingslinje. I Figur 2 visas det stora antalet e-postbrev med injektioner som utbyttes under övningen.



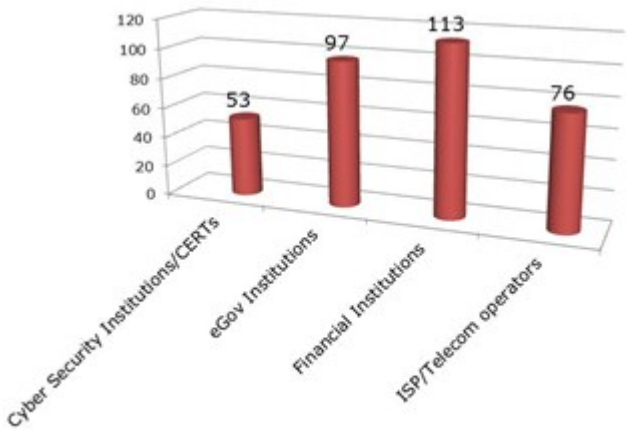
E-post-injektioner – CE2012

Figur 2: E-post-injektioner som skickades ut under övningen

Aktörerna

Övningsscenariot omfattade många olika aktörer. Sammanlagt 571 personer från 339 organisationer i Europa deltog i övningen. Tjugofem länder spelade med i övningen och även EU-institutioner. De deltagande organisationerna kom från följande grupper: organ och organisationer med ansvar för

it-säkerhet, berörda ministerier, leverantörer av e-förvaltningstjänster, finansinstitut samt internetleverantörer och operatörer av telekommunikationstjänster. Fördelningen av aktörerna visas i Figur 3.



Figur 3: Fördelning av de organisationer som deltog aktivt i CE2012

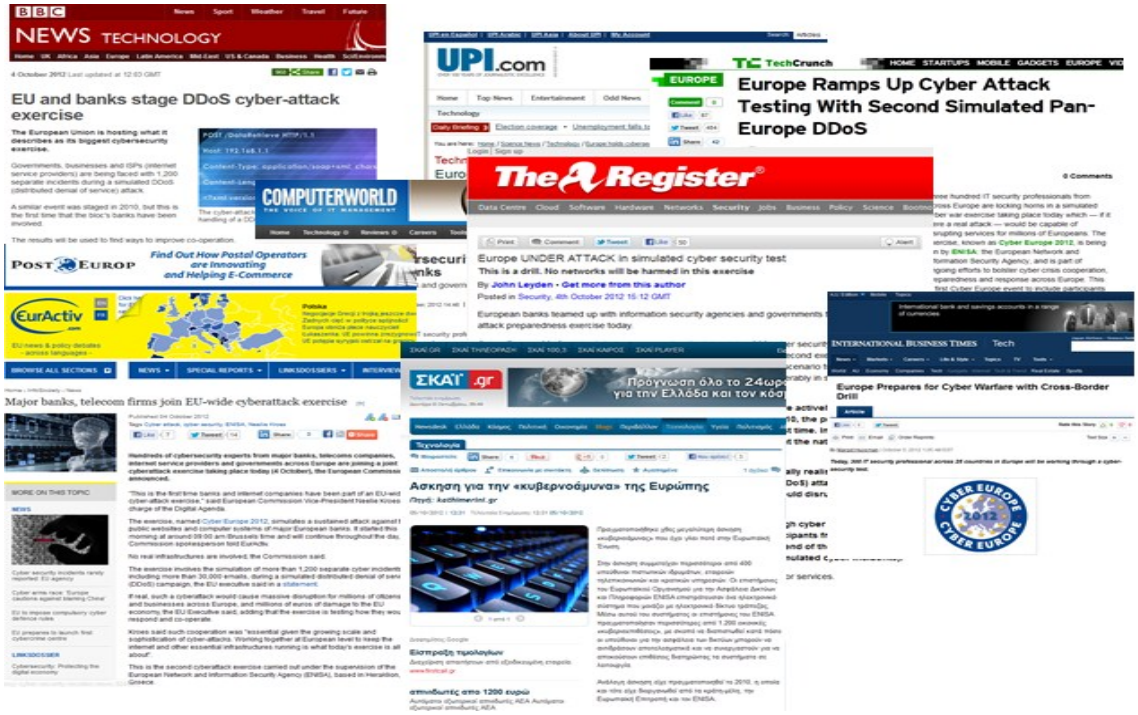
EN	*SV*
Cyber Security Institutions/CERTs	It-säkerhetsinstitutioner / incidenthanteringsorganisationer (Cert)
eGov Institutions	e-förvaltningsinstitutioner
Financial Institutions	finansinstitut
ISP/Telecom operators	internetleverantörer/telekomoperatörer

Medietäckning

Cyber Europe 2012 uppmärksammades stort i medierna världen över. Fler än 600 artiklar publicerades på 19 språk.

Många artiklar citerade kommissionens vice ordförande Neelie Kroes, kommissionsledamot med ansvar för den digitala agendan, som sade att ”samarbete på EU-nivå för att hålla igång internet och annan viktig infrastruktur är det dagens övning handlar om”.

Dessutom nämndes Cyber Europe 2012 i de sociala medierna på fler än sex språk. I sammanställningen av mediebudskap i bilden nedan visas några av de artiklar som publicerats om Cyber Europe 2012.



Huvudsakliga resultat

Cyber Europe 2012 ledde till en rad viktiga resultat när det gäller samarbete på nationell och internationell nivå och it-övningar. Resultaten sammanfattas nedan:

Samarbete på nationell nivå

- De deltagande länderna tog it-säkerhetshändelser på mycket stort allvar och besvarade utmaningarna genom att trappa upp sina nationella krishanteringscentrum och/eller genom att aktivera nationella krishanteringsstrukturer.
- Samarbetet och informationsutbytet mellan offentliga och privata aktörer på nationell nivå var intensivt under övningen.
- En del länder fick problem med beslutsprocessen i krishanteringen, även om den punkten inte ingick i övningsmålen (en del av de relevanta besluten måste till exempel fattas på mer strategiska nivåer under en kris).
- De offentlig-privata samarbetsstrukturerna skiljer sig åt mellan länderna. Parallella och ibland överlappande offentliga och privata förfaranden på nationell nivå ställde ibland till problem i det offentlig-privata samarbetet inom länderna.
- Deltagandet av organisationer från den privata sektorn på nationell nivå i övningen var en mycket positiv förbättring jämfört med den föregående Cyber Europe-övningen.

Samarbete på internationell nivå

- Cyber Europe 2012 har visat sig vara ett utmärkt tillfälle att undersöka, skapa förståelse kring och utvärdera befintliga europeiska it-samarbetsmekanismer Övningen har bidragit till att stärka och föra samman aktörerna inom hantering av it-säkerhetsincidenter i Europa.

- Alla deltagande länder var fullständigt delaktiga i övningens internationella samarbetsfas. Under övningen skedde många bilaterala och multilaterala utbyten på internationell nivå.
- En uppsättning operativa standardförfaranden och kommunikationsverktyg ingick i övningen, som gav struktur åt och skapade situationsmässig medvetenhet under den simulerade it-krisen.
- Problem konstaterades i de operativa förfarandena, särskilt när det gällde skalbarheten till följd av det stora antalet deltagande länder och institutioner.
- Kännedom om förfaranden och informationsflöden visade sig vara avgörande för att bygga upp en snabb och effektiv insatsförmåga i Europa.
- Lämpliga och aktuella tekniska infrastrukturer och verktyg visade sig också vara en nyckelfaktor för att garantera ett effektivt samarbete.
- Cyber Europe 2012 bidrog till att bygga upp förtroendet mellan länderna, vilket är en avgörande faktor för effektiva begränsningsåtgärder i rätt tid under verkliga it-kriser. Övningen har främjat både nya och befintliga förbindelser.

It-övningar

- Aktörerna inom hantering av it-säkerhetsincidenter i Europa anser att Europatäckande övningar är ett viktigt verktyg för att utvärdera och förbättra de befintliga samarbetsramarna vid it-kriser.
- Cyber Europe 2012 visade sig vara ett ytterst effektivt verktyg för att testa nationella beredskapsåtgärder och beredskapsnivåer.
- It-övningar är dessutom mycket användbara för att bygga upp förtroende mellan olika it-sammanslutningar.
- Effektiv planering är avgörande för att genomföra en så effektiv, storskalig och komplex övning som Cyber Europe.

Rekommendationer

Cyber Europe 2012 ledde till följande rekommendationer:

- Cyber Europe 2012 har visat sig vara ett värdefullt verktyg för att stärka den Europatäckande hanteringen av it-säkerhetsincidenter. Det är därför viktigt att fortsätta insatserna och vidareutveckla it-övningarna på europeisk nivå. EU-medlemsstaterna och Eftaländerna bör samarbeta för att genomföra nya Europatäckande och nationella it-övningar med målsättningen att stärka den gränsöverskridande hanteringen av it-säkerhetsincidenter. Vägledningen om god praxis för nationella övningar (Good Practice Guide on National Exercises)[1], som tagits fram av Enisa, ger ytterligare stöd på det här området.
- I framtida it-övningar bör man utforska sektorsöverskridande beroendeförhållanden och fokusera mer på särskilt utvalda grupper.

[1] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises

- Cyber Europe 2012 gav tillfälle till samarbete på internationell nivå och till att stärka samarbetet mellan aktörerna inom hantering av it-säkerhetsincidenter på europeisk nivå. För att främja internationellt samarbete är det viktigt att underlätta utbytet av god praxis om it-övningar, lärdomar, sakkunskap och anordnande av konferenser. Detta kommer att stärka de berörda aktörernas förmåga att hantera gränsöverskridande it-kriser.
- EU-medlemsstaterna och Eftaländerna bör ytterligare förbättra effektiviteten och skalbarheten hos och kunskapen om befintliga mekanismer, förfaranden och informationsflöden för samarbete på nationell nivå och med andra offentliga myndigheter i Europa. De lärdomar som dragits av Cyber Europe 2012 är en utmärkt utgångspunkt för det arbetet.
- Alla aktörer inom det internationella samarbetet om it-kriser bör utbildas i användningen av förfarandena så att de vet hur de ska arbeta med dem på effektivast möjliga sätt.
- Deltagandet av organisationer från den privata sektorn i övningen gav mervärde. EU-medlemsstaterna och Eftaländerna bör därför överväga att göra den privata sektorn delaktig i framtida övningar.
- Hanteringen av it-säkerhetsincidenter i Europa kan stärkas genom bidrag från andra viktiga sektorer i Europa (t.ex. hälsa och transport), som är relevanta för hanteringen av storskaliga kriser.

Mer information om samarbete kring it-kriser och övningar finns på Enisas webbplats på http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation

P.O. Box 1309, 71001 Heraklion, Grekland
www.enisa.europa.eu