PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4164 di Lunedì 29 gennaio 2018

Come l'Europa potenzia la lotta agli attacchi informatici

Gli strumenti che possono permettere alle squadre di intervento di emergenza e alle forze dell'ordine, di rendere più sicuri i sistemi informativi in caso di attacchi informatici e più incisiva l'attività repressiva e preventiva delle forze dell'ordine.

La European Union agency for network and information security - ENISA è un centro di riferimento e di eccellenza per le competenze nel campo della sicurezza informatica e delle reti, sia a livello europeo, sia a livello privato.

L'attività principale di questa agenzia è quella di sviluppare raccomandazioni e indicazioni su modalità sicure di protezione delle informazioni. Essa offre anche assistenza agli Stati membri nel produrre una legislazione appropriata e per migliorare la resilienza delle infrastrutture informatiche critiche europee contro attacchi malavitosi.

Questa azienda lavora a stretto contatto con numerose altri organismi, che hanno la stessa funzione, come ad esempio il CERT nazionale italiano e belga, e in particolare lo CSIRT - computer security Incident response Team.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[BIA0001] ?#>

L'attività di questi organismi si è sviluppata ulteriormente, dopo aver esaminato le conclusioni che sono state tratte dall'ormai famoso attacco con il virus chiamato Wannacry, che ha messo in evidenza come occorra un'operazione sinergica di tutte le autorità coinvolte, per fronteggiare queste tipologie di attacchi.

Gli aspetti tecnici, in particolare gli strumenti e le metodologie usate, rappresentano una componente importante in questa cooperazione.

Il documento, che riportiamo in allegato, è stato sviluppato proprio per supportare la cooperazione tra i vari enti coinvolti nella lotta al crimine informatico. Questo documento mette in evidenza alcuni aspetti tecnici della cooperazione, identifica delle aree di vulnerabilità e avanza raccomandazioni, atte a migliorare la situazione esistente.

I dati raccolti confermano che CSIRT e le forze dell'ordine scambiano sì informazioni durante la gestione delle indagini afferenti ad incidenti informatici, sia in maniera formale, sia informale, ma che occorre inquadrare questo scambio di informazioni in un quadro più organico.

È evidente che gli obiettivi di CSIRT e quelli delle forze dell'ordine possono essere diversi ed utilizzano strumenti diversi per raccogliere e trattare informazioni. Tuttavia, sta migliorando in maniera significativa il livello di mutua comprensione fra le due entità coinvolte, e il documento pubblicato sottolinea l'importanza di questa evoluzione.

Un punto sottolineato in questo documento fa riferimento al fatto che occorre stabilire uno scambio di informazioni impostato in maniera sistematica, invece che basato sulla disponibilità di uomini di buona volontà, operanti nei due enti.

Si può comunque intervenire con relativa rapidità, soprattutto perché alcune difficoltà, legate al miglioramento della cooperazione, sono più di natura legale organizzativa che tecnica.

In sintesi, il rapporto raccomanda quanto segue:

- tutte le agenzie europee coinvolte devono unire le loro forze per costruire e mantenere un archivio centralizzato di strumenti e metodologie, e formulare procedure, che possano facilitare la cooperazione tra i vari enti,
- tutte le agenzie europee coinvolte devono unire i loro sforzi per mantenere e arricchire un archivio centralizzato dei modelli di cooperazione tra le agenzie stesse,
- le forze dell'ordine devono mantenere una lista aggiornata dei relativi punti di contatto, indicando, dove possibile, quali sono i responsabili addetti al collegamento con altri enti,
- tutte le agenzie coinvolte devono definire i casi individuati nella piattaforma TIP ? Threat Intelligence platform, migliorando e rendendo più rapido lo scambio di informazioni.

Mi auguro che i lettori possano dare un'occhiata al documento allegato, perché molte delle raccomandazioni avanzate sono applicabili anche a livello di aziende private.

Allegato (82.3 Mb)

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it