HORIZON 2020

Enterprises intangible Risks Management via Economic models based on simulatioN of modErn cyber-aTtacks

Risultati in breve

Metodologie e strumenti per valutare meglio le vulnerabilità e proteggere i beni aziendali dagli attacchi informatici

Le imprese hanno il 28 % di probabilità di incorrere in una violazione dei dati di almeno 10 000 archivi, con conseguenti danni a beni immateriali come la reputazione, i diritti di proprietà intellettuale, le competenza e il know-how. Un'iniziativa dell'UE ha esplorato gli aspetti economici della sicurezza informatica per ovviare alla mancanza di informazioni quantitative da parte dei responsabili decisionali nel dare priorità agli investimenti nella sicurezza.

ECONOMIA DIGITALE

SICUREZZA

© NicoElNino, Shutterstock

Nel 2018 il costo stimato di una violazione dei dati è salito a 3,5 milioni di euro rispetto all'anno precedente, con un aumento di circa il 6,8 %. La maggior parte delle aziende adotta ancora una strategia basilare di risanamento, poiché le violazioni dei dati possono costare meno delle misure di sicurezza preventive. Inoltre, la misurazione dell'impatto reale degli incidenti in relazione ai costi necessari per il pieno recupero è un compito impegnativo. In generale, i modelli attuali sono inadeguati.

Il progetto finanziato dall'UE HERMENEUT consente alle organizzazioni di

valutare meglio la loro esposizione ai rischi informatici e l'impatto che gli attacchi informatici potrebbero avere sui beni di un'organizzazione, stimando le potenziali perdite finanziarie. «Abbiamo prestato particolare attenzione a beni quali la reputazione, il capitale umano e il marchio», spiega Paolo Roccetti, ricercatore senior e team leader della società coordinatrice del progetto, Engineering Ingegneria Informatica. «Abbiamo mantenuto le cose abbastanza semplici in modo che anche le organizzazioni con scarse conoscenze di sicurezza informatica possano usare la soluzione proposta».

Il team di HERMENEUT ha sviluppato una metodologia e uno strumento di supporto alle decisioni per valutare e quantificare le potenziali conseguenze economiche degli attacchi informatici sui beni di un'impresa e le perdite connesse ai suoi beni immateriali. Lo strumento di valutazione del rischio open-source integra i modelli e le conoscenze create durante il progetto. Fornisce agli utenti nuove funzionalità per facilitare la stima dei costi materiali e immateriali di un attacco, nonché un'analisi dei rischi, un'analisi basata sui costi e una valutazione delle contromisure adeguate per la protezione.

Sostenere valutazioni sulla sicurezza informatica olistiche e più semplici

Un altro risultato innovativo è stato l'approccio olistico per analizzare il rapporto costi-benefici della sicurezza informatica e il raggiungimento di molti obiettivi chiave nella lotta contro gli attacchi informatici. Tra questi, lo sviluppo di un modello di valutazione migliorato per le vulnerabilità organizzative e i rischi ai beni materiali e immateriali, nonché un modello dei costi per identificare e misurare i costi immateriali per le organizzazioni.

La soluzione HERMENEUT è stata progettata per supportare le decisioni in materia di sicurezza informatica dei responsabili della sicurezza informatica, dei dirigenti e dei membri dei consigli di amministrazione di un'ampia gamma di aziende, dalle PMI alle grandi organizzazioni. «Ciò rende le entità aziendali autonome nello stabilire un'attitudine informatica di base senza gli enormi costi di una valutazione dei rischi effettuata da un consulente, spesso troppo complessa per essere ri-eseguita e aggiornata», riferisce Roccetti. L'attitudine informatica è la misura della resilienza di un'azienda alle minacce alla sicurezza informatica.

Promuovere una cultura della gestione del rischio

Infine, i partner del progetto hanno delineato una serie di raccomandazioni politiche sui modelli economici dei costi connessi agli attacchi informatici, sulle soluzioni di gestione del rischio e su come sfruttare le migliori pratiche esistenti. L'obiettivo è quello di informare i responsabili politici europei e le altre principali parti interessate,

come le autorità di regolamentazione, gli operatori di mercato e le compagnie di assicurazione, sulle priorità fondamentali in questo settore e in quali ambiti l'Europa dovrebbe investire.

Protagonista chiave nella trasformazione digitale di aziende e organizzazioni pubbliche e private con circa 11 000 professionisti in 65 sedi nel mondo, Engineering Ingegneria Informatica, con sede in Italia, sta facendo tesoro dei risultati del progetto. Sta cercando di portare questa soluzione sul mercato.

«Grazie a HERMENEUT, le singole organizzazioni e i vari settori aziendali hanno ora a disposizione una suite di strumenti per migliorare la valutazione delle vulnerabilità degli attacchi informatici e dei beni materiali e immateriali a rischio», conclude Roccetti. «Aiuteranno anche i responsabili decisionali a stimare il rischio informatico e a capire quali mitigazioni adottare».

Parole chiave

HERMENEUT, attacco informatico, sicurezza informatica, beni immateriali, vulnerabilità, violazione dei dati, rischio informatico, valutazione del rischio, gestione del rischio

Scopri altri articoli nello stesso settore di applicazione

Promuovere la conservazione digitale a lungo termine dei dati scientifici

Modelli, metodologie e strumenti TIC, per migliorare la resilienza climatica e idrica delle città

Tecnologia Blockchain per pagamenti sicuri, a basso costo e semplici per tutti

Far esplodere i pozzi trivellati in modo più sicuro

Informazioni relative al progetto

HERMENEUT

ID dell'accordo di sovvenzione: 740322

Sito web del progetto

DOI
10.3030/740322

Progetto chiuso

Data della firma CE
26 Aprile 2017

Data di avvio
1 Maggio 2017

Data di completamento
30 Giugno 2019

Finanziato da
Secure societies - Protecting freedom and security of Europe and its citizens

Costo totale
€ 2 007 692,50

Contributo UE
€ 2 007 692,50

Coordinato da
ENGINEERING - INGEGNERIA INFORMATICA SPA
Italy

Ultimo aggiornamento: 20 Dicembre 2019