GLOBAL CYBER SECURITY CENTER

Global Cyber Security Center
La Fondazione di Poste Italiane

Milano, 13 ottobre 2016

Fondazione Global Cyber Security Center di Poste Italiane

Filoni di attività 2016

GLOBAL CYBER SECURITY CENTER

Progetti in corso (1/2)

Descrizione

Online Frauds Cyber Centre and Expert Network (OF2CEN): La Fondazione sta seguendo i lavori di manutenzione e sviluppo finale della piattaforma dello scambio informazioni polizia/banche sulle transazioni finanziarie fraudolente

E-Crime: Il progetto propone uno studio sul cyber crime atto a identificare quali siano i reali impatti socio-economici del fenomeno e quali possano essere le contromisure più idonee a contrastarlo. Alle controtmisure verrà poi associata una metodologia per calcolarne il costo

Enhancement of cyber educational system of Montenegro (ECESM): progetto per il rafforzamento del programma educativo sulla cyber security sia a livello accademico, sia a livello imprenditoriale sia per i cittadini in Montenegro. Il progetto prevede una serie di linee guida, un programma di alta formazione e l'erogazione di alcuni corsi di formazione

ATM – a look at the future and emerging security threats landscape: progetto volto alla pubblicazione di un white paper che descrive le minacce cyber presenti e future sugli ATM e le potenziali contromisure che possono essere prese in considerazione per la loro protezione

NATO Industrial Advisory Group 206: progetto volto alla classificazione dello stato dell'arte delle tecnologie di cyber situational defense awareness presenti nei Paesi membri NATO. Il lavoro è svolto assieme ai partner dell'industria difesa dei suddetti Paesi, divisi in 3 gruppi di lavoro: gruppo strategico, operativo e tecnologico

Progetti in corso (2/2)

Descrizione

Advanced Persistent Threat: studio su tecniche, tattiche e procedure avanzate di attacco con relativa metodologia di condivisione informazioni fra più enti e pubblicazione finale dei lavori. Lo studio è volto a sensibilizzare i Chief Information Security Officer a creare competenze di threat intelligence all'interno delle loro strutture e ad agevolare lo scambio informazioni attraverso standard riconosciuti a livello internazionale

Campagna sensibilizzazione cittadini: attività dedicata alla sensibilizzazione dei cittadini attraverso una esposizione di pannelli formativi e alla distribuzione di una pubblicazione sull'utilizzo sicuro di internet durante il mese della sicurezza (ottobre). L'evento, in collaborazione con Poste Italiane e la Polizia Postale ha l'obiettivo di illustrare i pericoli della rete ai cittadini (furto di identità, transazioni fraudolente,…)

Survey sul nuovo regolamento europeo sulla privacy: attività dedicata alla comprensione di quali possano essere gli impatti e le aspettative delle principali organizzazioni sia pubbliche sia private relativamente all'adozione del nuovo regolamento. La survey verrà divulgata pubblicamente attraverso l'osservatorio Europrivacy e pubblicata all'interno del rapporto CLUSIT

European Electronic Crime Task Force: coordinamento delle attività della European Electronic Crime Task Force, gruppo di lavoro fondato da Poste Italiane, Polizia Postale e US Secret Service. Sviluppo del sito della Task Force e organizzazione dell'evento plenario di novembre

Manifesto - Coordinated Vulnerability Disclosure: partendo dalla esperienza olandese, la Fondazione vuole promuovere un meccanismo di cooperazione fra più aziende ed esperti del settore per la divulgazione responsabile di informazioni su vulnerabilità tecniche di sicurezza che affliggono i servizi digitali delle aziende stesse

Programma eventi

SAS Forum
Data Scientist Story Telling
Milano

Attacco cyber
Esperienze operative per la resilienza del business
Roma

ATM
A look at the future and emerging security threats landscape
Roma

Information Resilience
come valore che guida l'innovazione
Milano

Evento EECTF
Casi reali di attacchi APT Modelli di attacco
Roma

aprile | maggio | giugno | luglio | agosto | settembre | ottobre | novembre

Manifesto
High Level Meeting Cyber Security
Amsterdam

Dream IT
Information Security – le sfide future e i problemi di sempre
Roma

Cyber Security Congress
Information security: fail often in order to succeed
Sibiu

Campagna sensibilizzazione
per il cittadino nel mese della cyber security
Roma

= speech effettuati

= eventi GCSEC

Collaborazioni

Canali di comunicazione di GCSEC

Commenti

- La newsletter è completamente in inglese
- Il bacino di utenti a cui è indirizzata è di circa 3.000 contatti a livello mondiale
- GCSEC prevede la possibilità agli addetti al settore di inserire un proprio intervento all'interno della newsletter

Alcuni partner che aderiscono

SecurityBrokers – Global Cyber Defense & Security Services · IBM · LUTECH · f5 · bsi.

Canali social attivi

628 followers

525 followers
4.500 visualizzazioni

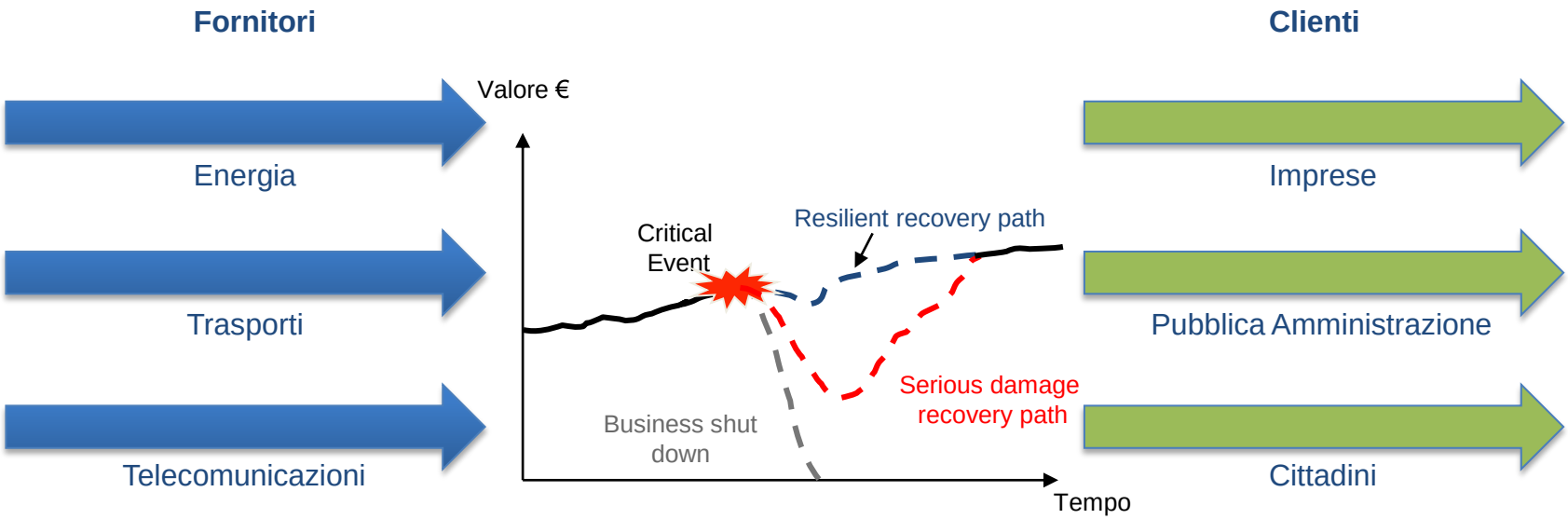
Iniziativa 2017

- La Fondazione collaborerà con il **CLUSIS** svizzero nella redazione della rivista Cybersecurity Trends
- La rivista uscirà trimestralmente, tradotta in 4 lingue: italiano, francese, tedesco e romeno
- La rivista includerà il punto di vista di esperti internazionali del settore

Global Cyber Security Center

La resilienza

Resilienza: Capacità di un materiale di assorbire un urto senza rompersi.



Questioni spesso aperte durante una crisi

- La gestione del fattore umano: come vengono assicurate le comunicazioni , il supporto e la mobilitazione di impiegati, manager, clienti e fornitori?
- In caso di assenza prolungata di energia, difficoltà di trasporto o viaggio, vengono garantiti approvvigionamenti sufficienti per mantenere gli uffici aperti? Vengono considerate soluzioni alternative quali il telelavoro? Esiste un piano di ottimizzazione dei consumi per permettere alle attività core di proseguire?
- Per quanto riguarda il business, vengono considerati i picchi di attività in base agli orari? i bacini geografici di clientela maggiori a cui garantire i servizi? E quali di questi servizi sono quelli maggiormente indispensabili per i nostri clienti?

Gli strumenti per essere resilienti

Conoscere il proprio business e la supply chain

Identificare i propri obiettivi di business e valutare il ruolo dei fornitori nel loro raggiungimento

Gestione dei rischi

Avere una piena consapevolezza e una corretta gestione dei rischi a cui l'azienda è soggetta per garantire il raggiungimento degli obiettivi di business

Monitoraggio

Monitorare costantemente l'infrastruttura e i servizi in cerca di anomalie/vulnerabilità/eventi considerando il contesto in cui si opera

Business Continuity

Mettere in atto processi, procedure e tecnologie a garanzia della continuità del business (piani di continuity, disaster recovery, …)

Gestione Incidenti e Crisi

Garantire una elevata capacità di difesa attraverso attività di prevenzione, reazione e analisi incidente, definizione dei piani di gestione crisi

Formazione e awareness

Formare e sensibilizzare il personale per ridurre i rischi legati al fattore umano

GLOBAL CYBER SECURITY CENTER