CYBER SECURITY. FONDAZIONE CRT, AL VIA PROGETTO-PILOTA IN ITALIA PER LA SICUREZZA INFORMATICA DEL TERZO SETTORE

- **Per la prima volta una fondazione bancaria italiana offre al non profit competenze e tecnologie all'avanguardia contro i cyber attacchi: sperimentazione su 300 associazioni**
- **Sfida connessa alla sicurezza del Paese, che subisce il 9,6% dei crimini informatici mondiali: in Italia attacchi cresciuti del 40% nel 2023, +300% in 5 anni**

Foto, video e materiali al link: https://vcloud.ilger.com/cloud14/index.php/s/G5J7dJLaxnXisnP

Le associazioni non profit vanno "a scuola" di sicurezza informatica con il pionieristico progetto "**SOS! Cyber Security**", ideato e sostenuto **per la prima volta in Italia** dalla **Fondazione CRT** per proteggere il patrimonio digitale degli enti del Terzo Settore e aumentarne la consapevolezza del rischio di cyber attacchi.

Cultura, welfare, salute, istruzione, ricerca, ambiente: in tutti questi ambiti i dati raccolti dal non profit rappresentano una grande risorsa per la collettività, ma costituiscono anche un bersaglio allettante per i criminali informatici. Trappole sempre più sofisticate sono capaci di trarre in inganno gli utenti. Utilizzo di password deboli, click su link pericolosi o compromessi, impiego di dispositivi non protetti, download di allegati e file da fonti sconosciute, condivisione di dati personali con fonti esterne, apertura di e-mail di phishing: **la stragrande maggioranza degli attacchi cibernetici è il risultato di errori umani**, con una percentuale che va dal **74% al 95%**[1]. Dati "monstre" che possono essere ridotti con percorsi di formazione mirati e l'implementazione dei controlli di sicurezza.

Con il progetto-pilota "SOS! Cyber Security" – realizzato in collaborazione con l'Associazione Next-Level e il partner tecnologico HRC – la Fondazione CRT è la prima fondazione di origine bancaria italiana a offrire gratuitamente al non profit **competenze e tecnologie all'avanguardia** contro i cyber attacchi, rispondendo a una sfida strettamente connessa con la **sicurezza nazionale**.

Secondo gli ultimi dati del Clusit-Associazione Italiana per la Sicurezza Informatica, infatti, nella prima metà del 2023 **l'Italia ha subito il 9,6% dei crimini informatici mondiali**. Gli attacchi sono aumentati del **40%** rispetto al 2022: una percentuale quasi quattro volte superiore a quella globale (11%). Considerando gli ultimi 5 anni, la crescita italiana è stata addirittura del **300%,** a fronte del 61,5% a livello globale.

In dettaglio, gli enti non profit riceveranno sia una **formazione tecnica specifica** sui temi della *security awareness* con il supporto della piattaforma di training on line per il riconoscimento delle minacce, sia un **pacchetto gratuito di strumenti avanzati di protezione** per i computer "targato" Cyberbrain, eccellenza torinese della cyber security: "Cyberdrive", una piattaforma articolata a più livelli per la condivisione sicura dei file nel completo rispetto della normativa GDPR

(Regolamento europeo in materia di protezione dei dati personali); servizi gestiti di rilevamento e risposta incidenti (MDR); antivirus proattivi e "intelligenti" per monitorare i dispositivi tramite centrale operativa presidiata da specialisti in cyber security. È previsto inoltre un **sistema automatico di backup** sicuro dei dati criptati all'origine presso il Datacenter di proprietà OGR Torino (Centro Dati certificato Tier III Certification Uptime Institute).

Potranno beneficiare del "cyber security kit" gratuito della Fondazione CRT **circa 300 organizzazioni non profit** del Piemonte e Valle d'Aosta, a partire da quelle che hanno partecipato oggi alla presentazione del progetto alle OGR Torino: un primo momento formativo con esperti di cyber sicurezza, cyber avvocati e vertici della Polizia Postale del Piemonte e Valle D'Aosta impegnati nel C.O.S.C. (Centro Operativo Sicurezza Cibernetica).

"*La Fondazione CRT intraprende una nuovissima sfida insieme alla Polizia Postale e in collaborazione con l'ecosistema dell'innovazione del territorio: promuovere la cultura della cybersicurezza nel Terzo Settore, per renderlo più consapevole e resiliente contro il rischio di attacchi informatici. La formazione del capitale umano e la protezione del patrimonio digitale sono un investimento per il futuro degli enti coinvolti e per la crescita dell'intera comunità, che trova nelle organizzazioni non profit la propria ossatura fondamentale*", afferma **Andrea Varese**, Segretario Generale della Fondazione CRT.

"*La Polizia Postale è la struttura specialistica della Polizia di Stato che si occupa del cyber crime in tutte le sue declinazioni, a partire dai cosiddetti cyber-attack fino alla protezione delle Infrastrutture critiche informatizzate. La rivoluzione digitale ha aperto nuove opportunità, ma ha anche favorito il diffondersi della criminalità online con un aumento esponenziale di reati nel periodo pandemico e nell'attuale situazione geopolitica caratterizzata dai conflitti bellici. L'impegno, pertanto, deve necessariamente essere corale, con una gestione proattiva dei rischi, una maggiore consapevolezza e nuove strategie e risorse a protezione di ogni realtà, da quella aziendale a quella privata*", dichiara **Manuela De Giorgi**, dirigente del C.O.S.C. Centro Operativo Sicurezza Cibernetica per il Piemonte e Valle d'Aosta.

Sempre secondo il Rapporto del Clusit, dal 2018 al primo semestre 2023 sono stati 505 gli attacchi di particolare gravità che hanno coinvolto realtà italiane: di questi ben **132** – ovvero il 26% – si sono verificati nel primo semestre 2023. La media mensile degli attacchi in Italia è passata da 15,7 nel 2022 a 22 nella prima metà di quest'anno. Per quanto riguarda la **tipologia di attacchi**, il **malware** (e in questa categoria il cosiddetto ransomware, che crittografa i file o impedisce di utilizzare il computer a meno che non si paghi un riscatto) continua a rappresentare la principale tecnica di attacco utilizzata dai criminali (**31%**), ma in modo molto meno consistente (era pari al 53% nel 2022) e di 4 punti percentuali inferiore al dato globale. Sono invece i **DDoS** (Distributed Denial of Service) – traducibile in italiano come interruzione distribuita del servizio, che consiste nel tempestare di richieste un sito, fino a metterlo ko e renderlo irraggiungibile – a registrare una notevole crescita, passando dal 4% del 2022 al **30%** del primo semestre 2023, una quota 5 volte superiore. Aumenta anche il dato degli attacchi di tipo **phishing** e ingegneria sociale, che in Italia incide in maniera maggiore rispetto al resto del mondo (14% a fronte dell'8,6% globale) (*https://clusit.it/rapporto-clusit/*).

[1] Secondo il report "ENISA Threat Landscape 2023", citato dal Rapporto Clusit 2023, il 74% delle violazioni ha coinvolto l'elemento umano (dati Verizon). Una percentuale che sale al 95%, secondo l'IBM Cyber Security Intelligence Index Report.