Comando
telefono 091 814 67 42 e-mail stampa@polca.ti.ch
url www.polizia.ti.ch

Repubblica e Cantone Ticino
Polizia cantonale
6501 Bellinzona

Comunicato stampa

SATI: una realtà in continua evoluzione

Bellinzona, 14.04.2023

Il concreto aumento dei cyber-rischi sia nell'ambito professionale sia nell'ambito privato è una diretta conseguenza della digitalizzazione della nostra società. Un fenomeno al quale le Autorità di polizia sono chiamate a rispondere adeguando i propri strumenti di contrasto. In questo senso, è previsto un rafforzamento della Sezione analisi tracce informatiche (SATI) della Polizia cantonale con l'integrazione di alcune figure professionali specialistiche.

Nel corso del 2022 la SATI ha sviluppato 31 inchieste (36 nel 2021), effettuato 101 (72) perquisizioni in supporto ad altri servizi, eseguito 1'026 (1'095) analisi informatico-forensi, elaborato 49 (45) analisi criminali operative, collaborato durante 25 (27) ricerche d'urgenza ed evaso 221 (250) richieste e-mail giunte da utenti o altre autorità. Inoltre, ha fornito un importante supporto alla Polizia giudiziaria e alla Gendarmeria nelle indagini classiche in cui vi erano delle componenti informatiche in gioco. Le attività illecite più frequenti riscontrate sono le truffe denominate *Business Email Compromise (BEC)*[1] – che hanno generato un danno economico di circa 1'260'000 franchi – e gli attacchi *ransomware*[2]. È stato inoltre osservato un aumento di reati in cui l'illecito profitto è stato incassato in cripto-valute.

In queste tipologie d'indagine, una delle difficoltà più grandi risiede nell'identificazione degli autori i quali, operando prevalentemente dall'estero, utilizzano espedienti che permettono loro di mantenere l'anonimato. Pertanto la collaborazione con le polizie estere risulta cruciale: in tredici occasioni la SATI ha infatti collaborato con le autorità estere in base alla Convenzione sulla criminalità informatica di Budapest (che fornisce una base giuridica per la cooperazione internazionale in ambito di indagini), per procedere alla conservazione di dati presenti su server di società ticinesi. Inoltre, un intervento scaturito da una richiesta di assistenza giudiziaria internazionale da parte delle autorità italiane ha portato alla perquisizione di una società situata nel Sopraceneri e al sequestro di alcuni server, nonché di materiale per l'acquisizione e distribuzione non autorizzata di segnali IPTV, tra i quali Sky e Dazn.

---

[1] I *BEC* prevedono, attraverso le tecniche del social engineering, l'accesso illecito a una casella di posta elettronica (solitamente aziendale) e la conseguente scoperta di una relazione finanziaria. I truffatori, spacciandosi quindi per il creditore o un dirigente dell'azienda, comunicano alla controparte delle false coordinate bancarie, sulle quali indirizzare il trasferimento fraudolento.

[2] Il termine *ransomware* (dall'inglese ransom = riscatto) si riferisce ad attacchi veicolati allo scopo di criptare i dati contenuti nei dispositivi, così da poter chiedere un riscatto in cambio della chiave di decifratura.

Un aspetto fondamentale resta la formazione, di base e continua, in ambito della cybercriminalità, della criminalità digitale e di quella legata all'evoluzione tecnologica. A questo proposito, lo scorso anno 34 ispettori e ispettrici di Polizia giudiziaria hanno conseguito la certificazione rilasciata dall'Istituto Svizzero di Polizia (ISP) nell'ambito della criminalità informatica. Inoltre, con l'obiettivo di rafforzare ulteriormente l'attività di contrasto a questi fenomeni, è in previsione l'inserimento di figure professionali specialistiche all'interno della SATI.

Quando l'anello debole della sicurezza informatica è il fattore umano, la prevenzione riveste un'estrema importanza. In particolare, vi sono alcuni accorgimenti che ogni utente può adottare per diminuire i rischi. Tra i tradizionali consigli vi è l'invito a diffidare delle e-mail ricevute senza sollecitazione e di cui non si conosce il mittente; a non dare seguito a richieste di pagamento; a usare prudenza se si ricevono e-mail che sollecitano un'azione da parte di chi le riceve e si minaccia altrimenti di conseguenze (perdita di denaro, querela penale, blocco del conto, disgrazia), a non aprire link e allegati in caso di e-mail sospette.
Un altro aspetto cruciale in questo ambito è la protezione degli accessi, fisici e virtuali: in quest'ultimo caso servirsi di password complesse, cambiandole regolarmente e utilizzando combinazioni diverse per i vari servizi online e, se possibile, attivare l'autenticazione a più fattori. Inoltre, un consiglio importante valido in tutti gli ambiti – ma in maniera specifica per le aziende – è mantenere costantemente aggiornati il sistema operativo e gli applicativi (ad esempio antivirus), effettuare delle copie di backup e investire coscienziosamente nella sicurezza della propria infrastruttura informatica e nella formazione dei propri collaboratori e delle proprie collaboratrici.

È possibile informarsi consultando i siti della Polizia cantonale www.polizia.ti.ch, del gruppo cantonale Cyber Sicuro www.cybersicuro.ch e della Prevenzione svizzera della criminalità (PSC) https://www.skppsc.ch/it/temi/internet/. Per quanto riguarda invece le segnalazioni è attivo il Centro nazionale per la cybersicurezza (NCSC) all'indirizzo https://www.ncsc.admin.ch/ncsc/it/home.html.

Contatto per i media:

Marco Montanaro, commissario capo, Responsabile della Sezione analisi tracce informatiche,
tel. 091 814 67 42, email stampa@polca.ti.ch