Le spese e gli sforzi per la sicurezza negli spazi pubblici aumentano

Delle misure come la giornata Clean-up vantano un sostegno incredibile da parte della popolazione, per esempio a Locarno. *Foto: IGSU*

La violenza giovanile, l'inquinamento acustico e il littering fanno parte della vita quotidiana di molti comuni. Secondo l'esperienza di Christoph Zulauf, direttore regionale a Berna e membro della direzione svizzera di Securitas SA, negli ultimi anni la situazione della sicurezza è cambiata in vari modi. «Nei comuni rurali la situazione è piuttosto stabile, mentre le conurbazioni affrontano in alcuni casi sfide considerevoli. Le autorità sono spesso confrontate con la violenza giovanile, il consumo eccessivo di alcol e il littering», spiega Luc A. Sergy, direttore dell'Associazione delle società svizzere di servizi di sicurezza (ASSS). Cifre concrete sull'evoluzione della situazione sono disponibili solo nella Svizzera romanda. Nel 2018, indica Luc A. Sergy, le spese per la sicurezza sono passate dal 7,8 al 21% a Bienne, dal 30,2 al 50% nel Canton Neuchâtel e dal 16,2 al 21% nel Canton Vaud.

Christoph Zulauf di Securitas ritiene che soprattutto nei comuni periurbani si dovrà lavorare in futuro su concetti di sicurezza per garantire la sicurezza negli spazi pubblici. Luc A. Sergy è d'accordo, «anche se la criminalità si sta spostando sempre più su Internet».

Non ridurre lo sforzo: questo motto vale anche per i rifiuti. I risultati dell'ultimo sondaggio condotto dal Gruppo d'interesse per un ambiente pulito (IGSU) e le cifre relative alle misure effettuate ogni anno da parte di IGSU dimostrano che il lavoro di sensibilizzazione e una fitta infrastruttura di raccolta sono efficaci contro il littering. Per il quarto anno consecutivo, la popolazione svizzera ha l'impressione che il littering continui a diminuire.

Anche molti comuni e città svizzeri notano un lieve miglioramento. Ad esempio, a Locarno, dove negli ultimi anni è stato dato maggiore spazio al lavoro di sensibilizzazione. «Dal momento dell'introduzione della tassa sui sacchi della spazzatura è aumentato anche il riciclaggio», afferma Christian Mora, responsabile dei Servizi pubblici della Città di Locarno. «Ciò ha anche un effetto positivo sul littering.»

Molte città e comuni si avvalgono inoltre sempre più spesso dei servizi di IGSU: delle offerte che stanno destando un interesse sempre più grande. «Delle misure come la giornata Clean-up vantano un sostegno incredibile da parte della popolazione», afferma soddisfatta Nora Steimer, direttrice di IGSU. «Le persone vogliono dare un contributo per un ambiente pulito e lo fanno durante il loro tempo libero.» In occasione della giornata Clean-up del 2019 sono state organizzate più di 650 operazioni di pulizia, per un totale stimato di circa 40 000 partecipanti alle giornate dedicate alla pulizia in settembre. Si tratta di circa 120 operazioni e 10 000 partecipanti in più rispetto all'anno precedente.

Anche i progetti di sponsorizzazione dei luoghi destano molto interesse. Nel 2018, IGSU ha lanciato un sito web, www.sponsorizzazionediluoghi.ch, che vuole sostenere gli organizzatori nella realizzazione di progetti di sponsorizzazione dei luoghi. Ciò ha convinto diversi comuni e città a realizzare i propri progetti di sponsorizzazione dei luoghi. Nel frattempo, sul sito si possono consultare progetti esistenti o nuovi di 23 diverse istituzioni. A ogni progetto hanno aderito fino a 80 padrini e madrine che ora ripuliscono volontariamente e regolarmente alcune aree dai rifiuti.

Fin dalla fondazione di IGSU 13 anni fa, i team degli ambasciatori IGSU percorrono le città e i comuni svizzeri coinvolgendo i passanti in colloqui sul littering e sul riciclaggio. Il loro lavoro di sensibilizzazione è apprezzato in tutta la Svizzera: nell'estate del 2019 si sono recati in oltre 50 città e 25 scuole, per un tale di 16 500 ore di lavoro di sensibilizzazione.

Tuttavia, il littering viene spesso usato come scusa per discutere l'introduzione di un deposito sui vuoti a rendere degli imballaggi per le bevande.

Tuttavia, tale deposito non risolverebbe in alcun modo il problema dei rifiuti. Solo il 7% degli oggetti abbandonati con noncuranza è costituito da lattine e bottiglie, che verrebbero restituiti a causa del vuoto a rendere. Il restante 93% verrebbe ignorato, visto che si tratta di mozziconi di sigarette, di imballaggi per cibo d'asporto, giornali, volantini, buste della spesa, sacchetti di patatine, vasetti dello yogurt, posate di plastica, ecc.

Inoltre, un deposito sui vuoti a rendere significherebbe inevitabilmente la scomparsa di tutti i punti di raccolta per alluminio, vetro e PET negli spazi pubblici, Lo smantellamento dell'infrastruttura di raccolta è controproducente. Quanto più facile è per la popolazione smaltire correttamente i materiali riciclabili e i rifiuti, tanto meno questi ultimi finiscono a terra. *fm/IGSU*

Cyberattacchi: i truffatori sfruttano la buona fede delle vittime

Quasi nessun attacco informatico funziona senza un certo grado di coinvolgimento delle vittime. Di solito infatti i truffatori dipendono dal fatto che, per esempio, la vittima fornisca una password, clicchi su un link a un sito web dannoso o apra un documento inviato per e-mail. Essi cercano quindi innanzitutto di acquisire quante più informazioni possibili sulle loro potenziali vittime. Queste informazioni vengono poi utilizzate per imbastire una storia plausibile, sostenuta da molti dettagli veri. Ciò rende l'e-mail inviata dai truffatori più credibile e aumenta la possibilità che la potenziale vittima commetta un errore. Il social engineering – ovvero l'atto di influenzare le potenziali vittime – può assumere forme diverse. Spesso la ricerca di informazioni da parte dei truffatori avviene online, senza che la vittima se ne accorga. Tuttavia, è anche possibile che un truffatore scopra che un dipendente comunale pratica nel tempo libero un determinato sport. Il truffatore cerca allora attraverso lo sport un contatto personale con la potenziale vittima, instaura un rapporto di fiducia e cerca così di ottenere informazioni.

Facendosi passare per il dirigente dell'azienda, i cybercriminali danno ordine al servizio finanziario di trasferire una grande somma di denaro. La prima vittima svizzera è stata una PMI del Canton Friburgo, che ha perso un milione di franchi svizzeri. *Foto: Shutterstock*

Alcuni anni fa i cybercriminali hanno scoperto un nuovo «modello di business», la cosiddetta «CEO Fraud». Facendosi passare per il dirigente dell'azienda, danno ordine al servizio finanziario della stessa di trasferire una grande somma di denaro. La prima vittima svizzera è stata una PMI del Canton Friburgo, che ha perso un milione di franchi svizzeri. Per proteggersi da tali attacchi, l'utilizzo di una firma collettiva dovrebbe essere previsto per i trasferimenti di denaro. Ciò implica che l'aggressore manipoli almeno due persone, il che è molto più complicato. Le informazioni interne, inoltre, non dovrebbero mai essere comunicate a sconosciuti. Infine, è indispensabile verificare con i superiori quando è espressamente vietato informare qualcuno dei «processi» dell'azienda. Una classificazione dei dati (ad esempio «interni», «confidenziali» e «segreti») definisce la sensibilità degli stessi e il trattamento appropriato. Nell'Amministrazione federale i dati classificati come «confidenziali» possono essere trasmessi unicamente per e-mail in forma criptata. I dati classificati come «segreti» possono essere trasmessi solo tramite corriere e devono essere memorizzati su dispositivi completamente isolati.

Max Klaus, capo sostituto della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI

Informazioni: www.ncsc.ch

Sensibilizzazione ai rischi

La Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)[1] 2018–2022 è stata approvata dal Consiglio federale nel maggio 2018. Il relativo piano di attuazione[2] e il piano di attuazione dei cantoni[3], che fa parte del piano nazionale, prevedono esplicitamente la sensibilizzazione ai cyber-rischi.

Grazie a una maggiore consapevolezza delle minacce provenienti dal cyberspazio è possibile indurre un cambiamento di comportamento degli utenti delle tecnologie dell'informazione e della comunicazione in modo che possano sfruttare pienamente le opportunità della digitalizzazione senza correre rischi evitabili.

Ulteriori informazioni per i comuni saranno disponibili nella seconda metà del 2020. La Rete nazionale de sostegno alle indagini nella lotta contro la criminalità informatica (NEDIK) sta elaborando attualmente con vari partner un corrispondente opuscolo informativo che sarà distribuito a tempo debito dall'Associazione dei Comuni Svizzeri.

[1] Organo direzione informatica della Confederazione ODIC (2018). Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022. URL: https://tinyurl.com/yattmmpk (stato: 30.03.2020).

[2] Organo direzione informatica della Confederazione ODIC (2019). Piano di attuazione della «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022»; URL: https://tinyurl.com/yaplwhpr (stato 30.03.2020).

[3] Rete integrata Svizzera per la sicurezza (2019). Piano di attuazione dei Cantoni. URL: https://tinyurl.com/y865da2k (stato 30.03.2020).