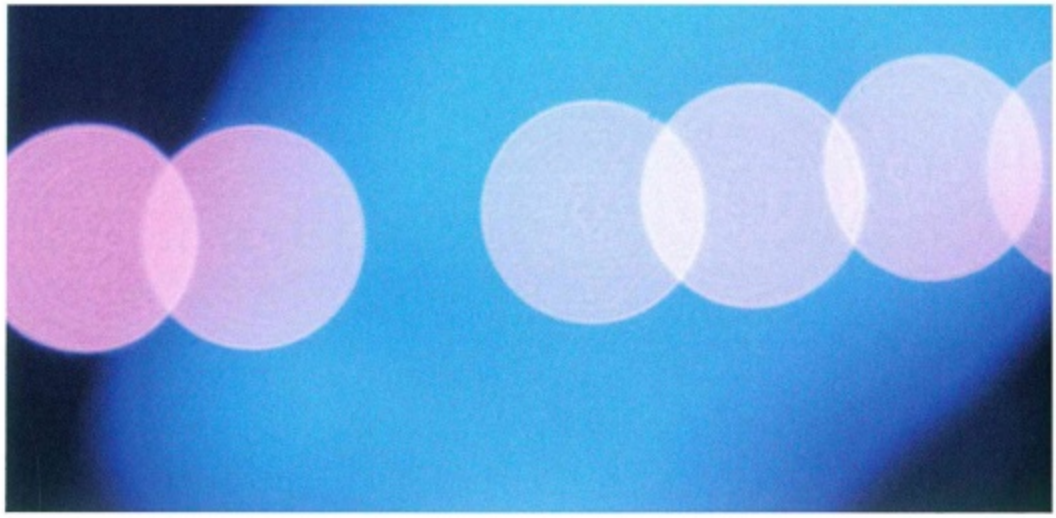
L'Editoriale

di Andrea Acito



Agosto 2021. ***Il mese degli ori olimpici, del green pass, degli europei di calcio, delle parole "ransomware", "cybersecurity", "hacker"*** *entrate nel lessico dell'italiano medio.*

L'1 agosto 2021, infatti, la Regione Lazio è colpita dal ransomware Ransomxx che cripta (blocca) dati critici, mettendo offline, anche il servizio vaccini COVID-19. Non è possibile ripristinare rapidamente il sistema perché l'Ente non aveva un backup off-site, ma solo online, che è criptato dallo stesso ransomware.

A settembre 2018, ero in un mirabolante hotel congressuale per partecipare ad un evento sulla cybersecurity. Si parlava di ***ransomware, tecniche di hacking, social engineering, infrastrutture IoT e privacy.***

Mi dirigo verso la sala dove è in corso la tavola rotonda "ISO27001 e GDPR", faccio una sosta al banco gadget, salto, con disinvoltura, la fila facendo miei una powerbank ed un paio di calzini. Il cellulare squilla...è il responsabile del servizio di assistenza, nome in codice "Winston Wolf". Penso:"nulla di buono!".

Io: "Ciao Wolf, tutto ok?". Wolf: "Luca, il collaboratore della società Galli, ha aperto un link in una mail. Tutti i file sono stati criptati, credo che si tratti di WannaCry...".

Wannacry è un ransomware che si diffonde grazie a finte mail e che dopo l'installazione su un computer infetta gli altri sistemi della rete. Cripta, quindi, i file rendendoli inaccessibili ed impedisce il riavvio del computer presentando una richiesta di riscatto.

Ci confrontiamo. Wolf controlla il back-up off-site che la società ha effettuato nel nostro datacenter, poi dice "ne abbiamo uno che risale a 10 minuti prima dell'attivazione del ransomware!"

Suggerisco di attivare un ambiente test per ***verificare il funzionamento del backup da cui creare un sistema failover. In 30 minuti è tutto on line*** *e dalla Galli possono collegarsi al cloud e riprendere il lavoro.*

Conclusione e lesson learned: ***che tu sia leone o gazzella... ops...volevo dire... non importa che sia Galli Srl o Regione Lazio... se hai il sospetto che nella tua organizzazione ci sia un signor Luca, fai sempre un backup off-line.***