Sistemi di sorveglianza e sicurezza

Il 7 febbraio 2019 è uscito sul Corriere della sera un articolo di Massimo Gaggi dal titolo “Usa, il business sicurezza nelle scuole”.

Dopo le stragi compiute da ragazzini nelle proprie scuole (la più famosa è quella della Columbine High School del 1999 con 15 morti; la più recente è quella di Parkland, con 17 morti), le contromisure non hanno portato alla riduzione delle armi da fuoco, ma all’aumento dei sistemi di videosorveglianza nelle scuole, con **migliaia e migliaia di telecamere.**

Con le dovute cautele, è possibile vedere alcuni parallelismi tra questa vicenda e alcune tendenze nell’ambito della sicurezza delle informazioni.

Prevenzione e rilevazione

Chiunque si occupa di sicurezza sa che le misure di rilevazione sono importanti, ma meno efficaci di quelle di prevenzione. Eppure le misure di rilevazione (telecamere, IDS, SIEM, vulnerability assessment e penetration test, processi di gestione degli incidenti) sono oggetto da sempre di maggiore interesse da parte dei venditori e degli utilizzatori delle misure di sicurezza.

Consideriamo solo **due esempi.** Il primo riguarda il NIST Cybersecurity framework, un insieme di 108 controlli di sicurezza pubblicati dal National Institute of Standards and Technology degli USA e adottati, tra gli altri, dalla BCE e dal “Framework Nazionale per la Cybersecurity e la Data Protection”. I controlli dedicati alla rilevazione e al trattamento degli incidenti e delle vulnerabilità (controlli di rilevazione e di recupero) sono più di 40 (più del 30%). Ad

essi vanno aggiunti altri controlli come quelli di verifica dell'integrità (PR.DS-6 e PR.DS-8). I controlli relativi alla configurazione sicura dei sistemi sono invece… uno (il PR.IP-1). Da questo punto di vista, sembra sicuramente meglio bilanciata la ISO/IEC 27001, che dedica 7 controlli su 114 alla gestione degli incidenti.

Il secondo esempio riguarda controlli di rilevazione come i *vulnerability assessment* e i *penetration test*, più pubblicizzati rispetto a quelli preventivi di configurazione sicura dei sistemi e di programmazione dei software da parte anche di persone qualificate. **Tre casi** tra gli altri:

- AgID e Accredia, per la qualifica dei servizi di conservazione, hanno promosso uno schema di certificazione delle società che vendono servizi di *vulnerability assessment* e *penetration test*, senza però promuovere schemi di certificazione delle competenze dei sistemisti, degli addetti alle reti e degli sviluppatori dei software;
- oggi lo schema di certificazione delle competenze degli "esperti di sicurezza" più riconosciuto è quello da Lead auditor ISO/IEC 27001, nonostante sia rivolto a persone addette alla verifica e non alla pianificazione e attuazione di un sistema di gestione per la sicurezza delle informazioni;
- relativamente alla sicurezza applicativa, il punto di riferimento più significativo è The OWASP™ Foundation (owasp.org); nella sua home page, i *Flagship Projects* (ossia i progetti ritenuti più significativi) sono 16 e più della metà di essi riguardano strumenti per identificare vulnerabilità, non per prevenirle.

Il caso della celebre OWASP Top ten è significativo: sebbene raccolga misure di prevenzione, è presentata inizialmente come strumento di identificazione delle vulnerabilità.

Come parlare (ma non usare) l’analisi del rischio

Nei supermercati è presente un gruppo ridotto di guardie addette alla prevenzione dei furti. Sicuramente i furti sono numerosi, ma non sufficienti per mettere in discussione il modello economico e organizzativo, per cui è evidentemente più conveniente la riduzione dei costi del personale rispetto alle perdite dovute ai furti. Nei supermercati sono comunque numerosi i dispositivi di videosorveglianza, necessari anche a dissuadere alcuni ladri.

Nel caso dei supermercati, l’analisi del rischio indica che il costo di ciascun evento è basso, anche se la probabilità è elevata. Questo giustifica l’uso delle misure di rilevazione (telecamere) e non di prevenzione (personale di vigilanza).

Nel caso delle stragi nelle scuole, l’analisi del rischio dovrebbe indicare che la probabilità di accadimento è bassa, ma le conseguenze sono altissime e questo dovrebbe portare a scegliere **misure di sicurezza diverse** rispetto a quelle da prevedere per probabilità alte e impatti bassi (per inciso, nel campo della sicurezza delle informazioni, nel caso di probabilità basse e impatti elevati, si preferiscono misure di recupero, come per esempio i backup e i siti di Disaster recovery; quando però sono in gioco vite umane è evidente che non si parla più di “sicurezza delle informazioni” e non è utilizzabile lo stesso schema; questo dimostra, ancora una volta, che ogni materia richiede una sensibilità diversa da quella richiesta da altre materie, anche se apparentemente simili).

I manager e il controllo

Chi prende le decisioni di spesa è un manager. E per un manager, per svolgere il proprio mestiere, il controllo è importantissimo. Lo dimostrano, tra le altre, le teorie

dedicate al controllo di gestione, la diffusione del "Management-by-objective" trasformato in "Management-by-measures" e la richiesta ossessiva di report da parte di tanti manager (questo, tra gli altri, ha portato all'introduzione di software gestionali molto complessi, ma anche molto problematici, in quanto l'obiettivo era quello di avere report senza pensare agli impatti sui processi).

Qui non si sta proponendo una critica alle pratiche di gestione delle organizzazioni; si sta solo richiamando l'attenzione su un atteggiamento tipico delle persone che hanno responsabilità all'interno di un'organizzazione. Questo atteggiamento è una delle componenti necessarie al loro ruolo: se non dovessero controllare alcunché, non sarebbero necessarie.

L'orientamento al controllo ha come effetto che i manager, dovendo scegliere, potrebbero preferire misure di rilevazione rispetto a quelle di prevenzione, anche se sono meno efficaci (non si spiegherebbe altrimenti l'introduzione, in alcune organizzazioni, degli inefficaci e inefficienti sistemi di *Data loss prevention*, che sono soprattutto sistemi di rilevazione).

Sfiducia nel prossimo e fiducia nei venditori

La vicenda del "controllo" delle armi nelle scuole mette in evidenza **due atteggiamenti contrapposti** ma presenti: il primo è la sfiducia completa nei confronti del prossimo, per cui è necessario armarsi di armi reali o di forme di controllo sempre più sofisticate, il secondo è la fiducia totale nei confronti dei venditori delle tecnologie, nonostante abbiano già dimostrato di potersene approfittare (si veda il caso di Cambridge Analytica).

I venditori di tecnologie hanno un vantaggio: vendono "soluzioni". Magari non sono efficaci, ma sono sempre

“soluzioni”. Un tempo era caratteristica degli informatici rispondere, ad ogni problema di sicurezza informatica, “ho un tool”; oggi sembra la risposta comune. Ancora più apprezzati sono i fornitori che propongono un “servizio chiavi in mano” (installazione della “soluzione”, sua manutenzione ed esercizio).

Conclusione

La **tendenza** è quindi sempre più quella di rifugiarsi in **tecnologie di controllo sempre più sofisticate**, complesse da mantenere e che lasciano sempre più spazio di manovra ai fornitori. Invece spesso basterebbe risparmiare su qualche gadget o consulente e investire di più in misure preventive, negli stipendi del personale che c’è già, nella sua formazione e nella sua crescita numerica. Questo permetterebbe anche di ridurre lo stress delle persone spesso costrette ad orari più lunghi del previsto e quindi gli errori. Dovrebbero però essere ridotti anche i super-fornitori, i super-consulenti e le super-tecnologie specializzate nella sorveglianza.

Riferimenti

L’articolo citato è disponibile online al seguente URL: https://www.corriere.it/editoriali/19_febbraio_07/usa-business-sicurezza-scuole-667de962-2afb-11e9-8bb3-2eff97dced46.shtml.

Il sito di OWASP è stato visitato il 12 marzo 2019.

Articolo a cura di **Cesare Gallotti**

Lavora dal 1999 nel campo della sicurezza delle informazioni, della qualità e della gestione dei servizi IT.

Ha condotto progetti di consulenza per la pubblica amministrazione e per il settore privato. Opera, sia in Italia che all’estero, come Lead Auditor ISO/IEC 27001, ISO 9001, ISO/IEC 200000 e ISO 22301. Ha progettato ed erogato corsi di

Quality Assurance e di certificazione Lead Auditor ISO/IEC 27001 e ITIL Foundation.

Tra gli attestati si segnalano: le certificazioni AICQ SICEV Lead Auditor ISO/IEC 27001, IRCA Lead Auditor 9001, CISA, ITIL Expert e CBCI, la qualifica come Lead Auditor ISO/IEC 20000 e il perfezionamento postlaurea in “Computer Forensics e investigazioni digitali”.

E’ capodelegazione del WG1 del comitato italiano ISO/IEC SC27 in UNINFO.

Ha pubblicato il libro, aggiornato nel 2017, “Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione; la norma ISO/IEC 27001:2013”.

Cura la pubblicazione, dal 2008, della newsletter “IT Service management news” (http://www.cesaregallotti.it/Newsletter.html).

Web: www.cesaregallotti.it; Blog: blog.cesaregallotti.it

https://www.ictsecuritymagazine.com/articoli/sistemi-di-sorveglianza-e-sicurezza/