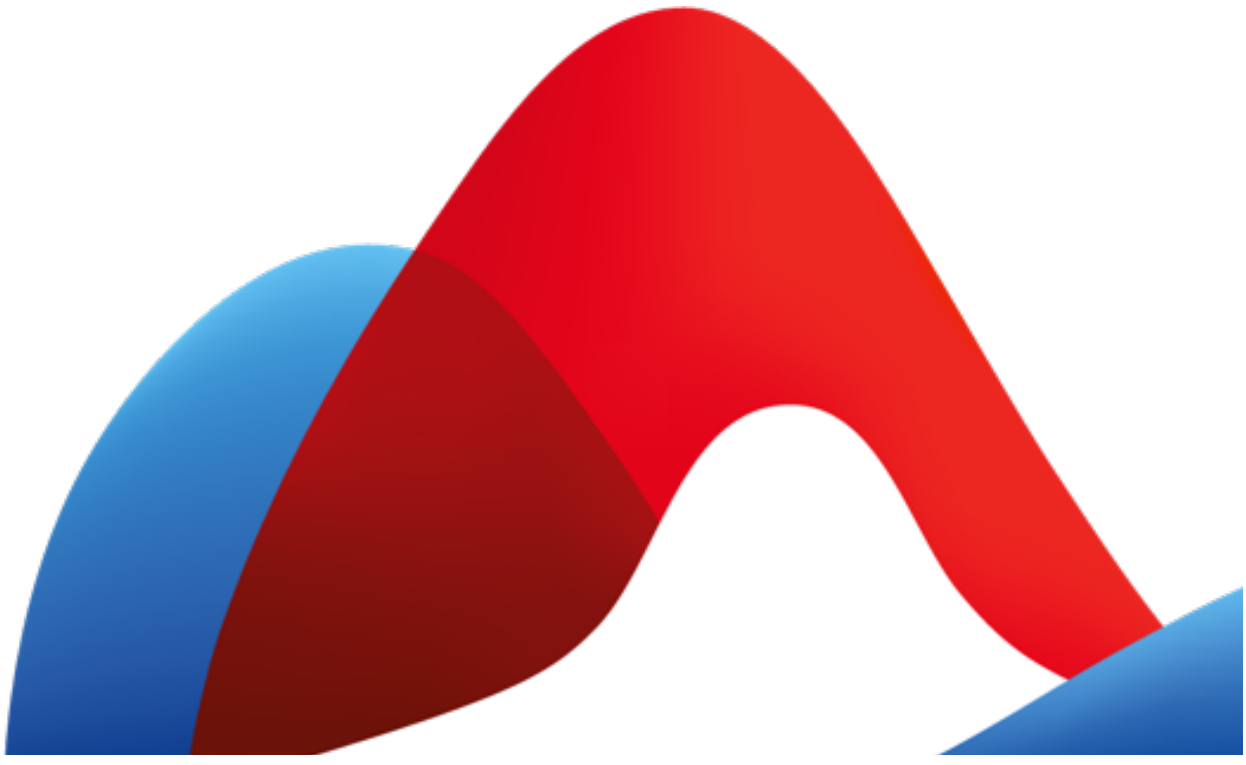
Cyber Security:

minacce attuali e relativa evoluzione

Autore
Dr. Stefan Frei, Security Architect, Swisscom

Agosto 2015



Indice

1 Introduzione 3

2 Evoluzione delle cyber-minacce 3

2.1 Quadro della situazione - Minacce sul radar 3

3 Minacce e progresso 5

3.1 Crescente complessità, società e internet 5

3.2 Dinamica delle innovazioni 8

3.3 Internet e macchine 9

3.4 Aggiornamenti automatici per la sicurezza 11

3.5 Vecchi sistemi (legacy) 11

3.6 Complessità dei software 12

4 Minacce e aggressori 13

4.1 Apparati statali e servizi segreti 14

4.2 Terrorismo 16

4.3 Criminalità organizzata 16

4.4 Hacktivisti 17

4.5 Vandali, script kiddie 17

5 Minacce e interconnessione della società 18

5.1 Disorientamento 18

5.2 Erosione della sfera privata 19

5.3 Erosione della fiducia 21

6 Riepilogo 21

7 Glossario 22

1 Introduzione

Nel corso degli ultimi due decenni lo sviluppo di nuove tecnologie, e in particolare di internet, ha creato opportunità incredibili, che hanno cambiato per sempre le nostre vite e che continueranno a cambiarle.
I cambiamenti scaturiti da internet possono essere considerati dirompenti. Hanno ripercussioni a livello globale, paragonabili a quelle della Rivoluzione industriale e di innovazioni come l'esplorazione dei giacimenti di petrolio, l'invenzione dell'automobile o l'introduzione degli antibiotici.
Sono oltre 3 milioni le persone che hanno accesso a internet, quindi il 42% della popolazione mondiale del 2014[1]. L'utilizzo di internet in mobilità presenta una crescita costante (il 95% della popolazione mondiale possiede un cellulare), proprio come il tempo medio trascorso quotidianamente online («always on»). La sicurezza in internet è diventata un fattore critico e la sua importanza cresce anche proporzionalmente all'interconnessione tra persone e dispositivi.
A livello sociale ed economico stiamo attraversando la fase iniziale dell'adattamento di queste opportunità. Ovviamente tali sviluppi comportano anche pericoli e minacce. Il settore della sicurezza in internet è caratterizzato da evoluzioni e cambiamenti rapidi che avvengono dove tecnologia, economia e società si incontrano.

In questa relazione presenteremo la situazione attuale delle cyber-minacce dal punto di vista di Swisscom e della Svizzera e, come principale azienda ICT svizzera, forniremo una stima sulla loro evoluzione nei prossimi 1-2 anni.

2 Evoluzione delle cyber-minacce

Internet unisce persone, macchine, tecnologia e società con un'intensità senza precedenti. Le opportunità, e le minacce che ne derivano, sono il risultato di innumerevoli innovazioni tecnologiche con relative applicazioni e servizi. Allo stato attuale il panorama delle minacce è complesso e in continua evoluzione. Nel presente documento non ci limiteremo a un excursus storico sulle minacce note o sulle singole tecnologie. Il nostro scopo è quello di valutare le minacce attuali sulla base delle dinamiche e degli sviluppi osservati, fornendone una presentazione alla luce delle evoluzioni attese nel corso dei prossimi 1-2 anni.

2.1 Quadro della situazione - Minacce sul radar

Le minacce hanno origine proprio nel continuo sviluppo delle tecnologie e del relativo uso e diffusione all'interno della società. Le potenziali minacce devono essere riconosciute precocemente e registrate sistematicamente. Per descrivere lo stato attuale delle

[1] Internet World Statistics - http://www.internetworldstats.com/stats.htm

minacce e la relativa evoluzione ci serviremo di un radar, mostrato nella Figura 1. I punti del radar rappresentano temi e minacce. I punti della Figura 1 rappresentano la situazione attuale. I segni più chiari mostrano l'evoluzione attesa per ogni minaccia nel corso dei prossimi 1-2 anni.

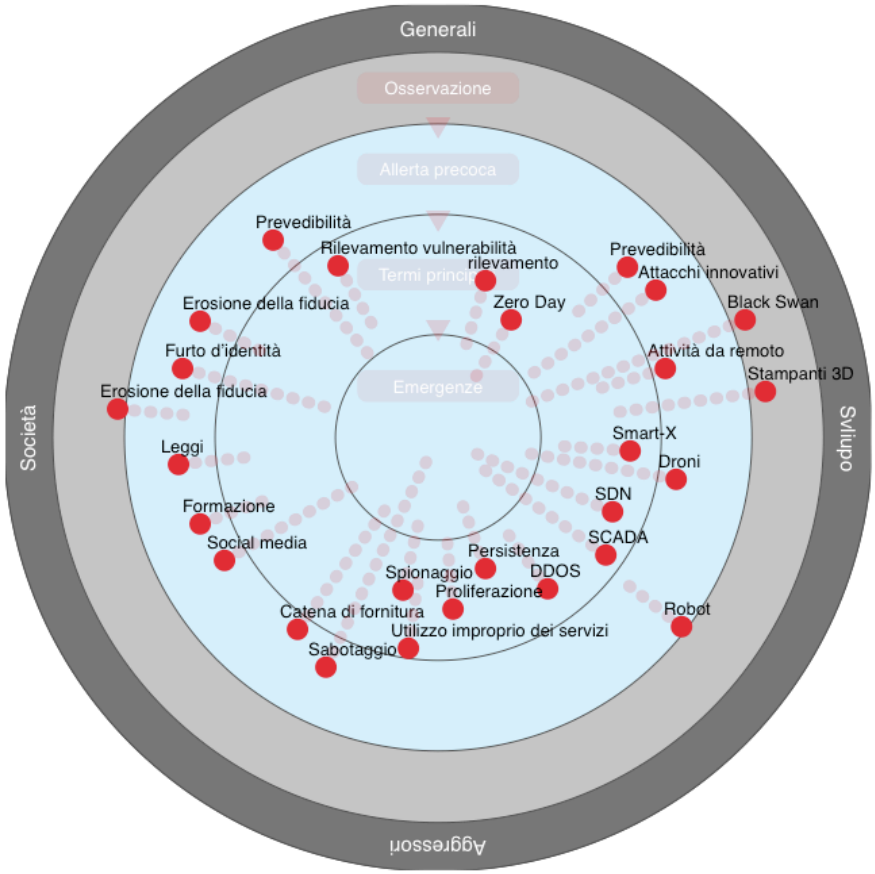


Figura 1 – Minacce al radar

La Figura 1 mostra che il radar è suddiviso in 4 diversi tipi di temi e minacce: *generali*, *sviluppo*, *aggressori* e *società*.

Sviluppo	Minacce derivanti dallo sviluppo tecnologico, che non vengono messe in atto da attori o aggressori specifici.
Aggressori	Minacce messe in atto dagli aggressori in modo mirato.
Società	Minacce che derivano dalla crescente interconnessione della società.
Generali	Minacce generiche che non possono rientrare in nessuna delle altre categorie o che rientrano in più di una categoria.

La suddivisione nelle categorie di cui sopra non è sempre netta.

Le nuove minacce, il loro riconoscimento, la valutazione e le contromisure seguono sempre un'evoluzione tipica che viene registrata nel radar secondo gli anelli concentrici *osservazione*, *allerta precoce*, *temi principali* e *urgenze*.

L'anello più esterno del radar è quello dell'*osservazione* e prevede la registrazione di temi e sviluppi che potrebbero trasformarsi in minacce. I temi dell'anello dell'*osservazione* vengono seguiti in modo sistematico, ma con risorse ridotte. L'anello dell'*allerta precoce* prevede la registrazione di minacce che potrebbero rivelarsi importanti nei prossimi anni. Queste minacce vengono studiate attivamente e in modo approfondito al fine di comprenderne al meglio i rischi e di preparare contromisure adeguate. Le minacce dell'anello *temi principali* sono quelle attuali e vengono introdotte delle contromisure attuate nell'ambito di regolari progetti e processi.

Se l'evoluzione e la gestione delle minacce avviene nell'ambito delle tre fasi descritte (*osservazione, allerta precoce, temi principali*), lavoriamo attivamente, quindi dal riconoscimento sistematico e precoce fino all'attuazione di contromisure concrete.

Per le minacce che ci colgono di sorpresa o quelle che si evolvono più rapidamente del previsto, la gestione è di tipo reattivo. E queste vengono inserite al centro del radar, nell'anello delle *emergenze*.

Il radar serve per avere una visione d'insieme, definire il quadro della situazione in modo sistematico e conoscere le evoluzione attese. Nel seguito approfondiremo le evoluzioni e le singole minacce.

3 Minacce e progresso

Innovazioni tecnologiche, nuove applicazioni pratiche, un diverso atteggiamento della società nei confronti di internet e un contesto diverso fanno sì che si presentino nuove opportunità e nuove minacce. Alcuni dei temi e delle minacce presenti nel radar derivano da processi o sviluppi sovraordinati.

3.1 Crescente complessità, società e internet

La nostra società odierna e l'utilizzo di internet hanno ormai ben poco in comune con gli anni attorno al 2000, quando scoppiò la «Bolla delle Dot-com». I prossimi anni potrebbero essere caratterizzati dalla stessa dinamicità e portare numerose innovazioni. La complessità del sistema internet e società aumenta costantemente e rapidamente, con un numero crescente di nuove modalità di interazione e combinazioni tra uomo, macchina, servizi e feedback. Parte di queste interazioni e combinazioni tra persone e macchine («devices»), che emergono ogni giorno e in grande quantità, aprono scenari di

attacco del tutto nuovi, che non sono prevedibili sulla base di considerazioni di carattere storico. Ciò significa che è necessario distinguere le minacce prevedibili e modellabili («more of the same») da quelle non prevedibili.

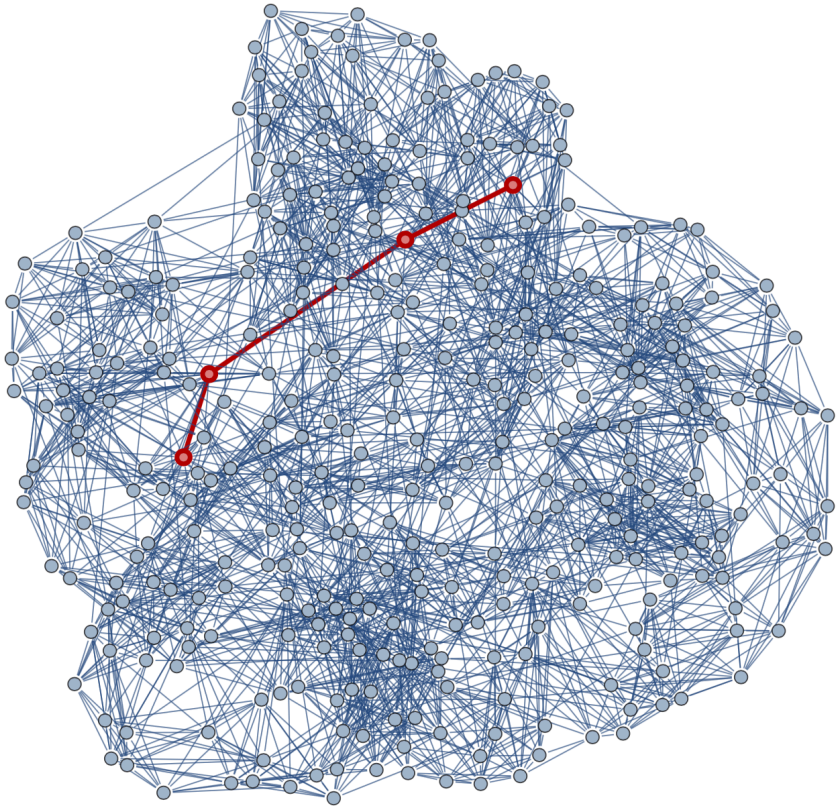


Figura 2 – Rappresentazione semplificata del sistema complesso internet e società. I nodi rappresentano le persone, le macchine, le applicazioni e i servizi che possono presentare interazioni diverse. Il numero delle nuove modalità di interazione (linee) tra i nodi subisce un aumento esponenziale per ogni nuovo nodo.

L'interconnessione crescente fa sì che al sistema internet e società si aggiungano costantemente nuovi nodi. Dall'elevato numero di nuove, e a volte sorprendenti, modalità di interazione che nascono ogni giorno, traiamo le seguenti informazioni sullo stato delle minacce:

Attacchi nuovi e innovativi	Aumenteranno gli attacchi qualitativamente nuovi, basati sulle nuove modalità di interazione. Tali attacchi fondamentalmente nuovi non saranno necessariamente avanzati dal punto di vista tecnologico. La scarsa protezione di base offerta ai sistemi di recente introduzione e la loro interconnessione, unite a una scarsa comprensione delle nuove interazioni create, consentono costantemente nuove e inattese modalità di attacco.

Prevedibilità	Diminuirà la prevedibilità degli attacchi. I riflettori sono attualmente puntati sulle tendenze e gli sviluppi come l'Internet delle cose, smart home, smart grid e così via, e sulle minacce che possono comportare.
Prevenzione	Le possibilità di attaccare sono sempre più varie e la prevenzione diventa più difficoltosa. Inoltre non è possibile prevedere gli attacchi qualitativamente nuovi. I sistemi e i servizi di sicurezza attuali possono proteggere solo dagli scenari per i quali sono stati concepiti.
Attività in remoto e a cascata	In un sistema complesso come quello illustrato nella Figura 2, sono collegati tra loro anche componenti ritenuti lontani tra loro e possono interagire anche in svariati modi. Ciò significa che un attacco a componenti di sistema anche lontani (o che prima erano isolati) possono improvvisamente influire direttamente su componenti propri. Inoltre è anche possibile che accessi di scarsa entità (o mossi da buone intenzioni) in un determinato punto del sistema portino a conseguenze gravi e impreviste in un altro punto («cascata»). Ci aspettiamo quindi che aumentino gli attacchi ai sotto-sistemi o ai fornitori allo scopo di compromettere un obiettivo primario. Riteniamo inoltre che piccoli errori o attacchi determineranno ancora più effetti a cascata tali da causare danni sorprendenti.

Esempio illustrativo di questi meccanismi
Tutti conoscono i dispositivi GPS e i loro vari utilizzi per la localizzazione. È meno risaputo che sono tantissimi i servizi critici e i dispositivi che dipendono da segnali GPS per conoscere l'ora esatta e per sincronizzare i processi. Un'interruzione involontaria o mirata del sistema GPS (es.: dovuto a un'attività solare estrema, a errori di configurazione o jamming) non comprometterebbe quindi solo i sistemi di navigazione.

Un esempio: nel 2007 a San Diego, negli USA, in seguito all'interruzione dei segnali GPS dovuta a un jamming non intenzionale, in tutta la città sono venuti a mancare per due ore i sistemi di telesoccorso, di telefonia cellulare, di gestione del traffico e i servizi bancomat.[2]

[2] http://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life.html

Da allora la dipendenza da GPS per l'indicazione dell'ora e la sincronizzazione di numerosi processi è anche aumentata. Sono innumerevoli i servizi che non sembrano collegati alla navigazione o alla localizzazione, ma che in realtà possono essere influenzati:[3]

- sistemi di comunicazione, telefoni, cellulari, reti di dati;
- sistemi di distribuzione dell'energia («power grid»);
- sistemi utilizzati per le transazioni finanziarie;
- sincronizzazione globale delle transazioni;
- sistemi e sensori distribuiti.

I possibili danni in caso di interruzione del segnale GPS sono scarsamente prevedibili e le interruzioni avrebbero un effetto a cascata. La prevenzione è estremamente importante, perché negli impianti fissi non è sufficiente ampliare la ricezione del segnale GPS.
Con il senno di poi è facile spiegare simili interruzioni, perché nel caso descritto i meccanismi di interdipendenza sono stati scoperti. Sarebbe comunque piuttosto complesso cercare di fornire un elenco di tutti i sistemi che dipendono dall'ora indicata dal GPS.

3.2 Dinamica delle innovazioni

Con la costante innovazione e il continuo miglioramento delle tecnologie esistenti in concomitanza con il crollo dei prezzi, si abbassa la soglia di accesso di diverse tipologie di attacco. La sicurezza che si basa

- sulla limitata disponibilità,
- sui prezzi elevati
- o sulle prestazioni limitate delle tecnologie adatte a mettere in atto gli attacchi,

è destinata ad andare in contro a un progressivo indebolimento nei prossimi anni. Ad esempio, quindi, sono attesi nuovi e sorprendenti attacchi e utilizzi legati alla disponibilità diffusa di stampanti 3D, droni, robot e così via.

Stampanti 3D	La sicurezza fondata sulla complessità o l'unicità di componenti meccanici si rivelerà inadeguata. Le chiavi o specifici strumenti meccanici si possono copiare o riprodurre più volte e con facilità. Spesso sostituire i componenti di sicurezza interessati risulta molto complesso e costoso, e non è possibile provvedere rapidamente o con un aggiornamento del software.

[3] http://www.gps.gov/applications/timing/

Droni e robot	Droni e robot in miniatura possono essere controllati a distanza superando così senza difficoltà le barriere di accesso. È necessario ripensare le attuali nozioni sulle barriere fisiche di protezione. Aumenteranno i casi di accesso a luoghi fisicamente inaccessibili al fine di pianificare degli attacchi. I sistemi che impediscono l'accesso a zone protette, ma permettono comunque di uscire liberamente all'esterno (es.: uscite di emergenza, sistema antincendio, uscite dei garage), sono facili da aggirare per robot infiltrati.
Software Defined Radio (SDR)	Con la diffusione delle Software Defined Radio (SDR), per gli aggressori sarà sempre più facile accedere ad ogni tipo di rete radio e di sistema di controllo. La presunta sicurezza data dall'utilizzo di protocolli non documentati si sgretola. La sicurezza basata sull'accesso privilegiato ad attrezzatura radio e bande di frequenza diventa così inadeguata. Aumenteranno gli attacchi ad ogni tipo di sistema di controllo a distanza e di comunicazione (veicoli, edifici, traffico, controllo accessi, WiFi, GSM, GPS, ecc.). Ad esempio oggi i jammer GPS costano poco meno di 100 USD.

3.3 Internet e macchine

Con le connessioni disponibili sempre e ovunque e la continua miniaturizzazione dei componenti, sono sempre di più le macchine, i dispositivi («devices») e i sensori che si possono collegare alle reti. Questo sviluppo si sta facendo strada rapidamente in diversi settori. Oltre ai sistemi di controllo che gestiscono i processi industriali e i flussi di energia, cresce la diffusione di dispositivi e sensori che agiscono sulla nostra quotidianità. Un ottimo esempio viene dalla svolta energetica cui si punta con le «smart grid», con la domotica delle «smart home», con il controllo intelligente del traffico e con le «smart car», ma anche con i dispositivi «wearable» e con la robotica. Con la crescente diffusione di queste tecnologie cresce anche il potenziale degli aggressori.
Malfunzionamenti e attacchi in internet causeranno sempre più danni non virtuali con conseguenze potenzialmente fatali per l'uomo, l'ambiente, la società e le cose. Grazie all'interconnessione, voluta o meno, dei dispositivi ci aspettiamo che nei prossimi anni gli attacchi in questo campo subiranno un incremento.

Sistemi di controllo industriale ICS/SCADA	Nell'ambito dei sistemi ICS/SCADA, le vulnerabilità e gli strumenti di attacco crescono più rapidamente della possibile protezione. Aumenteranno gli attacchi mirati e riusciti nei confronti di tali sistemi di controllo. La protezione di sistemi di controllo quasi del tutto chiusi e inaccessibili, che non dispongono di alcun meccanismo integrato per l'aggiornamento sicuro dei software, è impossibile o molto costosa. E poi l'utilizzo di questi sistemi di controllo è più esteso nel tempo rispetto a quanto avviene con i sistemi degli utenti come PC, tablet e telefoni cellulari. Molti dei sistemi di controllo critici sono ormai obsoleti e sono stati realizzati quando le minacce erano praticamente inesistenti rispetto a oggi. Questi sistemi sono quindi molto vulnerabili e potrebbero essere compromessi anche da attacchi molto semplici.
Smart home, smart grid, smart car, smart qualsiasi cosa	Concorrenza più forte, crollo dei prezzi e miniaturizzazione portano a una rapida diffusione di ogni tipo di sistema e dispositivo «smart». Spesso in fase di progettazione la sicurezza non è una priorità. • Scarsa consapevolezza su attacchi complessi-innovativi • Il «Time to market» è più importante della sicurezza • La sicurezza dei singoli componenti e dell'interazione tra diversi componenti continua a non essere compresa a pieno • Mancano le risorse per garantire con efficacia la sicurezza di dispositivi ad elevata miniaturizzazione L'utente finale utilizza poi questi sistemi per scopi innovativi, non previsti in fase di progettazione. Ciò fa sì che la protezione di tali sistemi di controllo o della loro comunicazione non sia sufficiente. Ci aspettiamo più attacchi e nuovi guasti eclatanti con danni di natura non virtuale.

3.4 Aggiornamenti automatici per la sicurezza

In uno scenario in cui le minacce sono in continuo aumento, la possibilità di aggiornare un sistema attraverso dei semplici aggiornamenti per la sicurezza assume un'importanza straordinaria. I produttori dei sistemi operativi e dei software più diffusi (Windows, browser, App Store, ecc.) ne sono consapevoli e hanno impresso una notevole accelerazione alla praticità e all'automatizzazione degli aggiornamenti per la sicurezza. La Figura 3 mostra l'andamento dell'evoluzione della minaccia insieme a quella della protezione offerta dagli aggiornamenti per la sicurezza di un normale computer. Con gli aggiornamenti per la sicurezza, la protezione viene costantemente adeguata alla minaccia.
Qualsiasi tipo di sistema di controllo (ICS/SCADA, Smart-X ecc.) che non disponga di qualche meccanismo per eseguire gli aggiornamenti per la sicurezza in modo semplice e veloce, sarà sempre vulnerabile. Come mostra la Figura 3, la minaccia cresce, la sicurezza intrinseca si sgretola. Ciò è acuito dal fatto che sistemi di questo tipo prevedono un utilizzo più prolungato nel tempo rispetto ai PC.

Efficaci meccanismi di aggiornamento per ogni tipo di sistema interconnesso sono un requisito irrinunciabile al fine di garantire sicurezza e durata.

In un prodotto o dispositivo interconnesso, la mancanza di meccanismi dedicati agli aggiornamenti automatici per la sicurezza è un chiaro indicatore di attacchi e guasti futuri.

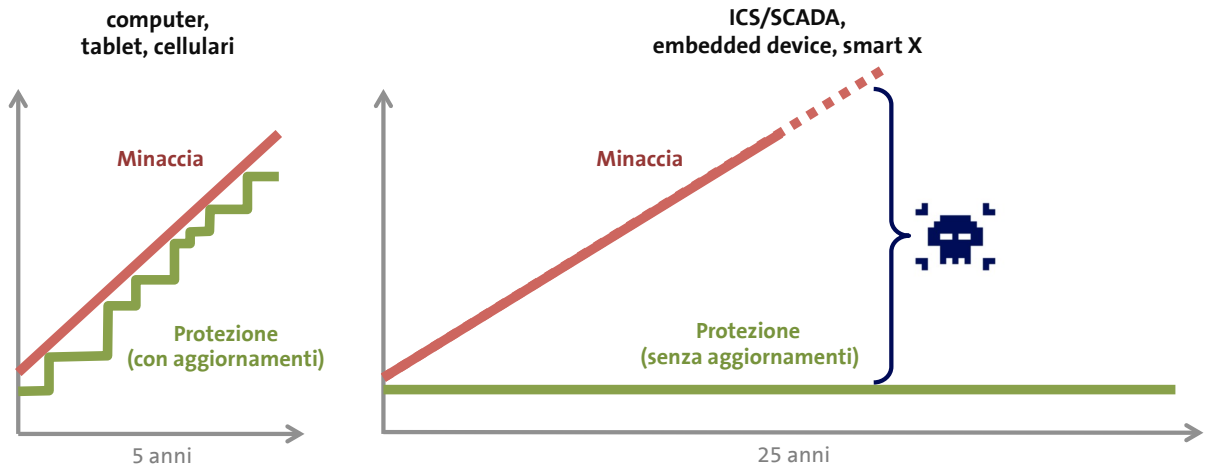


Figura 3 – Nei sistemi ICS/SCADA, il tempo di esercizio prolungato senza possibilità di aggiornamenti per la sicurezza determina un aumento costante della vulnerabilità.

3.5 Vecchi sistemi (legacy)

Sono molti i sistemi informatici, con le relative applicazioni, che vengono utilizzati per un periodo di tempo molto più lungo di quello previsto dal produttore. Per tali sistemi non è

più prevista l'assistenza del produttore e gli ambienti operativi e di sviluppo sono obsoleti, come i protocolli di comunicazione in uso. A ciò si aggiunge il fatto che non ci sono meccanismi di protezione integrati simili a quelli presenti sui PC (es.: antimalware, exploit mitigation, ecc.). Solitamente si tratta di sistemi complessi che svolgono funzioni critiche e specifiche: due delle ragioni per cui non vengono sostituiti.
Allo stesso tempo questi «sistemi legacy» sono però investiti dalla stessa ondata di interconnessione (molteplice, diretta e indiretta), sia esterna, che interna. La loro capacità di resistere agli attacchi rimane invariata, ma nel frattempo il pericolo continua a crescere, come mostra la Figura 3.

Sistemi e protocolli legacy	Ci aspettiamo più attacchi a sistemi e protocolli critici e obsoleti. Con la diffusione delle competenze tecniche su tali sistemi, aumenta il pericolo.
Interconnessione e API	I sistemi legacy, senza collegamenti diretti con l'esterno, vengono sempre più spesso collegati alle cosiddette interfacce API, mediante una moderna sovrastruttura. In questo modo i sistemi, i dati che contengono e funzioni che un tempo erano isolate, vengono esposti al mondo esterno. Ci aspettiamo un ulteriore aumento della diffusione di interfacce API e di strumenti di comunicazione e protocolli macchina-macchina, che aprono una faglia in settori che prima erano protetti. Ciò produce anche nuovi e innovativi vettori di attacco. Ci aspettiamo inoltre un maggior numero di «data breach», i dati di sistemi che prima operavano isolati saranno quindi esposti.

3.6 Complessità dei software

Nonostante i grandi progressi e investimenti nello sviluppo di software sicuri, il settore non è ancora riuscito a creare software che nascano sicuri e a metterli sul mercato. Sono solo 4 su 6 i grandi produttori di software che sono riusciti a ridurre le vulnerabilità dei loro prodotti nel corso dell'ultimo anno, rispetto alla media degli ultimi 5 anni. Figura 4 mostra l'andamento delle vulnerabilità dei software negli ultimi 20 anni.

Vulnerabilità dei software	Continuiamo ad aspettarci numerose vulnerabilità in tutti i software con una vasta quota di mercato. Tra questi troviamo sistemi che non vengono percepiti direttamente come computer, non fanno eccezione, ad esempio, i sistemi di controllo, SmartX

e sensori.

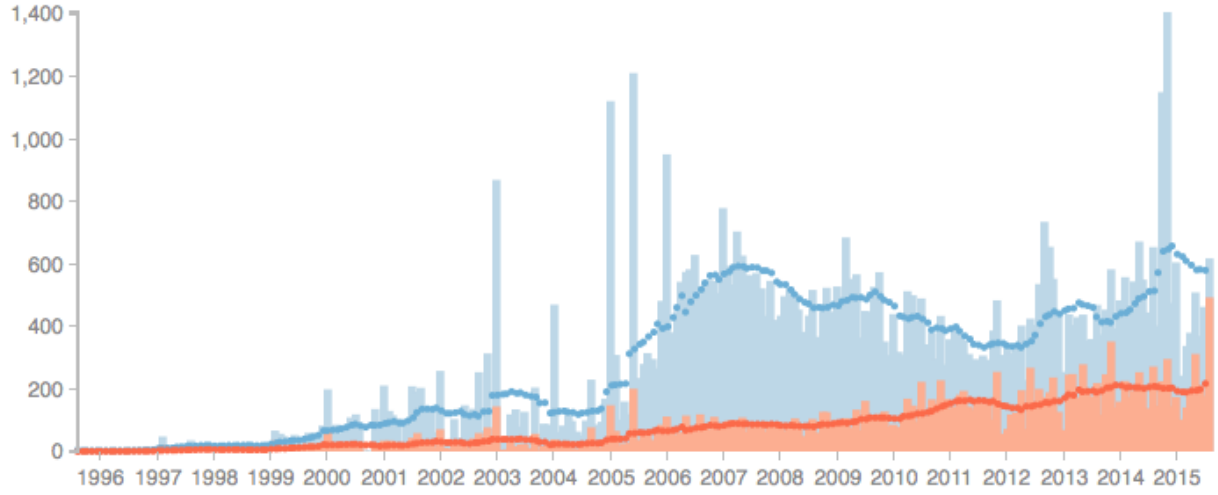


Figura 4 - Vulnerabilità rese note per mese, dal 1995 al 2015. In rosso: vulnerabilità dei primi 10 produttori. Le linee mostrano la media dei 12 mesi precedenti.[4]

Crescerà l'importanza di meccanismi di aggiornamento per la sicurezza che risultino efficaci, capaci di aggiornare in poco tempo un elevato numero di sistemi. In un prodotto o dispositivo interconnesso, la mancanza di meccanismi simili è un chiaro indicatore di attacchi e guasti futuri.

4 Minacce e aggressori

Le minacce descritte sopra sono il risultato dello sviluppo di internet, della tecnologia e della società, in assenza di uno specifico attore che pianifichi, diriga o metta in atto una minaccia.

Nella quarta parte descriveremo le minacce che provengono da aggressori.

Distingueremo 5 gruppi di attori con obiettivi, mezzi e procedure diverse. I gruppi sono elencati nella Figura 5.

[4] http://techzoom.net/BugBounty/SecureSoftware

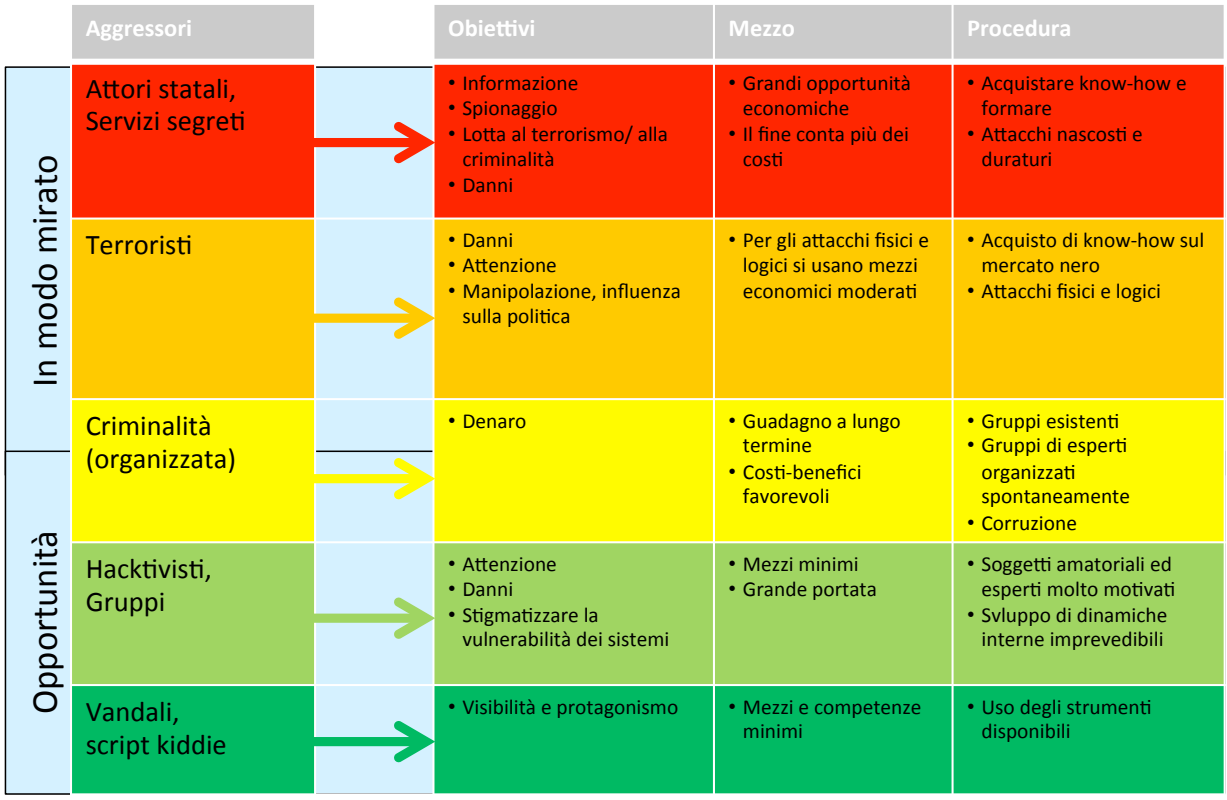


Figura 5 – Classificazione degli aggressori

Distinguiamo inoltre anche gli attori che sfruttano un'*opportunità* da quelli che agiscono in modo *mirato*, anche se il confine tra loro non è netto.

Opportunità	Attori che sfruttano le opportunità offerte da internet a fronte di una casualità o perché l'obiettivo è scarsamente protetto.
In modo mirato	Attori che perseguono con un obiettivo preciso con coerenza e spesso con risorse considerevoli (risorse economiche, competenze, personale, materiale). Sono solitamente persistenti, continuano a perseguire il proprio obiettivo anche per molto tempo e su più canali parallelamente.

4.1 Apparati statali e servizi segreti

Da sempre apparati statali e servizi segreti conducono operazioni di spionaggio e sabotaggio. Cyber-spionaggio e sabotaggio sono sempre più frequenti nelle strategie militari di attacco e difesa. Alcuni stati stanno ampliando notevolmente le proprie competenze informatiche proprio in questo settore.
A differenza dei criminali informatici e di altri aggressori, gli stati possono accedere direttamente a parti critiche dell'infrastruttura di internet («internet backbone») e

costringere per legge fornitori di servizi e produttori a forme di sorveglianza e collaborazione. Le attività condotte dagli stati vanno da un controllo sistematico e ampio di ciò che avviene in internet, all'introduzione segreta di malware nell'hardware e software dei sistemi target di altri paesi (o concorrenti).
L'obiettivo, da una parte, è quello di ottenere informazioni e, dall'altra, di creare dei varchi nascosti («backdoor», «kill switch») che permettano azioni di sabotaggio in caso di necessità. Nello specifico si intercettano dati in modo sistematico e diffuso in nome della lotta al terrorismo e del controllo degli oppositori.
Gli aggressori appartenenti ad apparati statali dispongono di enormi risorse e di un ampio margine di manovra che permettono loro di raggiungere i propri obiettivi con persistenza, su più canali e per periodi di tempo prolungati.

Catena di fornitura Supply chain	Dobbiamo partire dal presupposto che parti dell'infrastruttura critica del nostro paese sono già compromesse. In futuro l'integrità degli oggetti forniti dovrà affrontare sfide sempre maggiori e dovrà essere messa in discussione.
Spionaggio industriale	Nel nostro paese gran parte della creazione di valore deriva da diritti industriali e di proprietà intellettuale. Prevediamo un aumento degli attacchi finalizzati allo spionaggio industriale.
Sabotaggio/preparazione	I servizi segreti utilizzeranno più kill switch o altri preparativi per essere pronti a mettere in atto un sabotaggio in caso di necessità. Ciò riguarda sia hardware, che software. Si tratta di funzioni che, ad esempio, possono manifestarsi per «motivi di manutenzione» nelle «vulnerabilità dei software» o in nodi di accesso fissi e integrati. A volte è difficile stabilire che un determinato problema è frutto di una misura intenzionale di un avversario. L'hardware può anche essere stato fornito con meccanismi di sicurezza e punti di rottura predeterminati in modo che una determinata funzione possa essere attivata o disattivata a distanza mediante un impulso da software.
Telefonia mobile, WiFi	Le reti di telefonia mobile o WiFi subiscono sempre più attacchi attivi o passivi (sniffing, jamming, spoofing, SS7, ...).
APT/Zero Day	Aumenteranno gli attacchi tecnicamente sofisticati, che saranno al contempo più difficili da individuare.

4.2 Terrorismo

Proprio come i criminali, anche i terroristi sfruttano le opportunità offerte da internet. Il loro obiettivo tuttavia non è di tipo economico: essi puntano a ottenere l'attenzione o a ottenerne di più e a manipolare e influenzare politica e società. Quindi sono decisamente realistici gli scenari in cui mirano a causare quanto più danno possibile al fine di ottenere quanta più attenzione possibile, disseminando paura e terrore.

Utilizzo improprio dei servizi	Aumenterà l'utilizzo improprio di servizi consolidati per scopi di propaganda o reclutamento (ad es.: hosting, social media, comunicazione).
DDOS	Aumenteranno gli attacchi di tipo «Distributed Denial of Service» come dimostrazione di potere o gli attacchi capaci di causare danni estremamente elevati.
Eventi	Gli obiettivi dei cyber attacchi saranno sempre più spesso i grandi eventi o le conferenze su temi delicati. Così anche i fornitori di prodotti e servizi per tali eventi saranno sempre più colpiti.
Strumenti elettronici	Ci aspettiamo un aumento degli attacchi di ogni tipo mirati a strumenti elettronici (TV, radio, web, social media) che godono di grande seguito. Sono obiettivi perfetti per fare propaganda, diffondere la paura e dimostrare la propria forza.
Nodi critici	Ci aspettiamo più attacchi mirati a nodi critici molto popolari (Facebook, Twitter, blog, ecc.).

Grandi eventi o servizi che riguardano un pubblico molto vasto (es.: emittenti televisive, trasmissione di grandi eventi come i mondiali di calcio) sono le piattaforma ideale per attacchi terroristici. Oltre a questi servizi il pericolo interessa sempre più anche i nodi individuali (come Twitter, Facebook, ecc.) che permettono di raggiungere un grande numero di persone. Ci aspettiamo che tali servizi e nodi rientrino sempre più tra gli obiettivi di attacchi mirati.

4.3 Criminalità organizzata

La criminalità e la criminalità organizzata rientrano tra i più antichi fenomeni sociali e la storia ci insegna che i criminali si appropriano molto rapidamente delle nuove tecnologie e le sfruttano a proprio vantaggio.
Per raggiungere i propri obiettivi economici, i criminali operano in modo professionale, sia in modo mirato, che sfruttando delle opportunità.
Esistono diversi gruppi di criminali, specializzati in settori diversi, come ad esempio la ricerca di vulnerabilità, la creazione di malware, la vendita o il noleggio di strumenti, la gestione di botnet, il reclutamento di money mule, la creazione di e-mail di phishing e

così via. La criminalità tradizionale e quella informatica si integrano e si confondono tra loro.
Grazie a questa suddivisione del lavoro, i «servizi» e gli «strumenti» offerti in vendita o a noleggio ai soggetti interessati sono di qualità elevata.

Diffusione di strumenti e servizi (proliferazione)	Gli strumenti per mettere in atto un attacco e i servizi di gestione dei sistemi compromessi sono sempre più sofisticati e diffusi.
Attacchi complessi	Gli attacchi complessi e su più livelli (es.: deviazione DDOS) aumenteranno. Gli attacchi di phishing saranno psicologicamente più raffinati e perfettamente su misura della vittima in termini di aspetto, contenuto e tempistica («spearphishing»).
Mimetizzazione, impedimento della rilevazione	I malware e gli strumenti di attacco saranno sempre più abili nel sottrarsi al rilevamento da parte dei sistemi di sicurezza.
Persistenza	La ricerca e lo sfruttamento delle vulnerabilità saranno sempre più sistematici, gli attacchi verranno commercializzati e offerti ai potenziali acquirenti.

4.4 Hacktivisti

La missione degli hacktivisti è solitamente legata a temi emotivamente significativi. Il coordinamento della loro attività può concretizzarsi attraverso i social media (spesso in modo spontaneo) riuscendo in poco tempo a trovare e a riunire vasti gruppi di persone accomunate dalle stesse idee. L'obiettivo dell'attacco è determinato dal tema (nemici dell'ambiente, governi, aziende dominanti...) o scaturisce spontaneamente. Gli attori sono fortemente motivati e contano tra le proprie fila anche competenze professionali. È facile che all'interno del gruppo si facciano strada dinamiche incontrollabili.

Social media	Ci aspettiamo un aumento delle campagne spontanee o degli attacchi coordinati tramite social media contro obiettivi direttamente o indirettamente collegati al tema scatenante.

4.5 Vandali, script kiddie

I vandali e gli script kiddie sono aggressori non professionali, mossi da noia o da desiderio di protagonismo, che hanno facile accesso a strumenti che consentono loro di mettere in atto degli attacchi o di condurre «esperimenti». Non c'è un obiettivo specifico, si tratta di

ottenere visibilità grazie a un cyber-attacco con mezzi e competenze minimi. In questi casi gli obiettivi e il momento dell'attacco sono piuttosto casuali.
Attacchi del genere devono essere considerati e trattati come un rumore di fondo permanente su internet. La protezione di base di tutti i sistemi interconnessi deve essere in grado di proteggere automaticamente da simili attacchi. Con la maggiore disponibilità di informazioni e gli strumenti di attacco più semplici da utilizzare, questi attacchi non diminuiranno, la protezione di base deve essere soggetta a verifiche e adeguamenti costanti.

5 Minacce e interconnessione della società

5.1 Disorientamento

Le innovazioni tecnologiche e i nuovi utilizzi di internet sono caratterizzati da un'introduzione molto rapida. Gli attori di nicchia possono diventare soggetti dominanti nel giro di pochi anni, e ciò rappresenta una minaccia per i modelli aziendali conosciuti e per la sicurezza. È una situazione molto impegnativa per le persone e l'economia, perché interi rami possono essere messi in discussione da un giorno all'altro (es.: tassisti e Uber, hotel e AirBnB). Per natura, opporsi, nascondere o addirittura tentare di invertire tale sviluppo, non avrebbe molto successo nel lungo periodo.

«Because there is no army that can hold back an economic principle whose time has come»
John Donovan, AT&T

Continua ad esserci il pericolo che, come economia e società, non riusciremo a tenere il passo di internet, con la dinamicità che ha introdotto, nella ricerca del diritto e nella formazione - con conseguenze disastrose per le generazioni future.

Figura 6 – L'introduzione delle nuove tecnologie è sempre più rapida, ciò pone le persone e la società di fronte a grandi sfide.

Dobbiamo imparare in fretta a rapportarci adeguatamente a questa dinamicità e agilità dell'epoca di internet, su tutti i livelli. Per valutare correttamente i vantaggi e i rischi derivanti da sviluppi come il «cloud computing», la «shared economy», l'apprendimento a distanza e così via, dobbiamo cambiare il nostro modo di pensare. Se non vogliamo addentrarci inconsapevolmente in interdipendenze indesiderate, dobbiamo riconoscere precocemente i rischi e le opportunità e disporre di meccanismi che permettano di sfruttarne il potenziale.
Ciò che è conosciuto lascia spazio alla novità, ciò che abbiamo cambia in continuazione. Orientarsi in tanta varietà e in questo flusso di informazioni diventa più difficile.

Formazione	Il nostro sistema educativo continua ad essere improntato all'insegnamento di capacità, utile nelle prime fasi dell'industrializzazione.[5] Cresce il rischio di non essere in grado di stare al passo del progresso a livello sociale ed economico.
Politica, ricerca del diritto	La ricerca del diritto non riesce assolutamente a tenere il passo rapido degli sviluppi dell'era di internet. La conoscenza e la comprensione dei vasti scenari dell'ambiente virtuale sono rare, e il pericolo è che le leggi promulgate non siano adeguate o che al momento dell'introduzione siano già obsolete. Il dibattito in corso sui «software di intrusione» dell'*intesa di Wassenaar* è un ottimo esempio di questa sfida.[6]
Persone	Di fronte alla crescente complessità e varietà dei servizi, delle possibilità di interazione e combinazione, l'uomo si sente sempre più in difficoltà e affaticato. Ciò vale sia per gli amministratori di sistemi ICT, che per gli utenti finali. E fornisce nuovi margini di manovra agli aggressori. La complessità è il peggior nemico della sicurezza, sia dal punto di vista tecnico, che da quello umano e sociale.

5.2 Erosione della sfera privata

Per identificarsi rispetto a servizi e autorità, ogni persona dispone di un numero finito - e ridotto - di attributi personali. Il numero dei servizi internet che utilizziamo e utilizzeremo ogni giorno cresce costantemente. Ogni volta che si verifica una fuga di dati presso un

[5] https://www.youtube.com/watch?v=Optk-gYgFo8
[6] https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation

qualsiasi servizio o autorità, tutti gli attributi identificativi delle persone si perdono man mano. Attributi come *indirizzo e-mail*, *password* e *domande di sicurezza* sono semplici da cambiare in caso di fuga di dati. Ma cambiare gli attributi statici come ad esempio il *numero di assicurazione sociale*, la *data di nascita*, il *luogo di nascita*, il *sesso*, la *residenza* e così via, è (quasi) impossibile. Questo sviluppo, unito alla grande quantità di informazioni personali visibili sui social media («OSINT»), fa sì che gli attributi personali non potranno essere tenuti segreti nel tempo[7].

Sarà sempre più difficile proteggere i dati personali resi disponibili a terzi. Sono in aumento, sia in termini quantitativi che qualitativi, gli attacchi che simulano fiducia utilizzando dati privati e personali al fine di portare la vittima a compiere determinate azioni.

Furto di identità	Con la progressiva erosione della sfera privata, aumenteranno gli attacchi come il furto d'identità. Gli attacchi saranno più sofisticati (personali) e per le persone coinvolte sarà sempre più difficile riconoscerli, se non addirittura impossibile.
Utilizzo improprio dei dati	Il grande volume di dati personali e metadati, in continuo aumento, presso stati, terzi e fornitori di servizi fa crescere il pericolo di utilizzi improprio e monitoraggio.
Strada a senso unico	I dati personali, anche se forniti un'unica volta (volontariamente o meno), non possono essere ritirati. Basta una fuga di dati o un passo falso per compromettere *definitivamente* la sfera privata. Dobbiamo tenere presente che, a lungo termine, gran parte dei nostri dati personali (ad es.: contatti) non potranno essere mantenuti privati. Molte app, ad esempio, al primo avvio, chiedono all'utente di consentire l'accesso ai propri dati di contatto. Rispondendo «sì», anche una sola volta, non sarà più possibile tornare indietro e i dati di contatto non potranno mai essere ritirati.

[7] http://techzoom.net/Publications/Papers/databreach

5.3 Erosione della fiducia

Con il continuo flusso di informazioni e il crescente uso improprio di informazioni private e personali, la fiducia generale nei servizi e nelle informazioni si sgretola.

Erosione della fiducia	È sempre più difficile riconoscere gli attacchi che simulano la fiducia utilizzando dati personali e privati con metodi sofisticati. Questi attacchi aumenteranno e avranno sempre più successo.

6 Riepilogo

Inizialmente tutte le nuove tecnologie determinano incertezza. L'adattamento e il corretto utilizzo rappresentano pertanto un processo che richiede del tempo. Dobbiamo riconoscere quali rischi possiamo scongiurare individualmente (come utenti o organizzazioni), quali sono le minacce che derivano o nascono dal sistema e quali possano essere affrontate in modo sostenibile solo a livello sociale e con forme di collaborazione internazionali.

Da queste riflessioni si conclude quanto segue:

- la sicurezza in internet è prevalentemente un problema di gestione della complessità. Per comprendere le minacce non è sufficiente considerare solo la tecnologia.
- La prevenzione totale è un'illusione. Aziende e autorità devono partire dal presupposto che le proprie infrastrutture verranno compromesse (o sono già state compromesse).
- Le organizzazioni devono accertarsi che una compromissione riuscita possa essere individuata e mitigata nel minor tempo possibile.
- Una volta stabilita una compromissione è necessario procedere secondo un processo definito e appreso, e non in emergenza.
- In un prodotto o dispositivo interconnesso, la mancanza di meccanismi efficaci per gli aggiornamenti automatici dei software è un chiaro indicatore di attacchi e guasti futuri.
- Partiamo dal presupposto che gli attacchi mirati aumenteranno e che le loro modalità e tempistiche saranno ancora meno prevedibili.

7 Glossario

0-day/Zero-day exploit	Exploit di un software che è noto già da prima o dal momento in cui una faglia nella sicurezza viene resa nota. Ciò significa che l'exploit è disponibile da prima che i produttori del software abbiano predisposto una patch di sicurezza.
API	Application Programming Interface Interfaccia di programmazione che permette ai programmi di scambiarsi dati con un unico linguaggio (macchina-macchina).
Backdoor	Porta sul retro nell'informatica che permette di accedere a un computer aggirando le protezioni.
Botnet	Rete di cui fa parte un elevato numero di computer compromessi, controllati centralmente da un botmaster.
Defacement	Inserimento di contenuti indesiderati in una pagina web attaccata da hacker.
DOS, DDOS	Denial of Service (DOS) Malfunzionamento di un sistema causato da un elevato numero di richieste. Distributed Denial of Service (DDOS) Attacco DOS che parte simultaneamente da un elevato numero di sistemi distribuiti (ad es.: una botnet). Fermare l'attacco non è facile.
Exploit	Programma, codice o sequenze di comandi che permettono di sfruttare le vulnerabilità di un software.
Exploit Mitigation	Concetto generico che indica le tecniche utilizzate per ostacolare o impedire lo sfruttamento delle vulnerabilità dei sistemi.
GPS	Global Positioning System Sistema di navigazione satellitare utilizzato per la localizzazione e l'orario.
ICS	Industry Control System Termine generico che indica i sistemi di controllo industriale, vedere SCADA.
ICT	Information and Communication Technology, abbreviazione che indica il settore informatico e delle telecomunicazioni.
Jamming	Disturbo intenzionale delle telecomunicazioni.
Kill-switch	Software nascosto e in grado di reagire a ordini esterni. Disturba il funzionamento di un sistema o lo rende inutilizzabile.

Malware	Software che avvia attività dannose e indesiderate.
Money mule	Persone indotte ad accettare pagamenti dai «clienti» e a trasferire le somme di denaro, in cambio di una commissione. Il soggetto (money mule) è convinto di lavorare per un'organizzazione legittima.
OSINT	Open Source Intelligence Raccolta di informazioni con l'utilizzo esclusivo di fonti pubblicamente accessibili.
Patch Aggiornamento per la sicurezza	Codice che sostituisce il software difettoso per eliminarne le faglie nella sicurezza.
Phishing	Con il phishing gli utenti vengono indotti (perlopiù tramite e-mail con false richieste) a rivelare informazioni sensibili.
SCADA	Supervisory Control And Data Acquisition System Sistemi per il monitoraggio e il controllo degli impianti (ad es.: processi industriali).
Vulnerabilità	Faglie nella sicurezza o punti deboli di hardware o software che forniscono agli aggressori un punto di accesso al sistema.
SDR	Software Defined Radio Trasmettitore universale ad alta frequenza che genera il segnale da software, adattabile pertanto da parte dell'utente a diversi protocolli e applicazioni.
Smart grid	Rete elettrica intelligente Il concetto di smart grid comprende l'interconnessione e il controllo di generazione, stoccaggio e utilizzo di energia elettrica, nonché delle reti di trasmissione e distribuzione.
Smart home	Domotica Concetto che abbraccia il controllo in rete e parzialmente automatizzato di energia, manutenzione e sicurezza in edifici e appartamenti.
Social media	Siti web che permettono lo scambio tra gli utenti attraverso un profilo proprio (es.: Facebook, Twitter, LinkedIn, Xing).
Spearphishing	Attacchi di phishing mirati e personalizzati.
Spoofing	Tentativi di frode all'interno di reti al fine di nascondere la propria identità.