SICUREZZA DELL'INFORMAZIONE NELLE IMPRESE SVIZZERE

Uno studio sulle minacce,
il management dei rischi e le forme di cooperazione

Zurigo, agosto 2006

CSS
An ETH Center

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Contatto:
Center for Security Studies
Seilergraben 45–49
ETH Zentrum / SEI
CH-8092 Zurigo
Svizzera
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch

Indice

Elenco delle illustrazioni

Prefazione

La criminalità su Internet esiste da quando il computer ha soppiantato carta e penna. Da quando i computer sono stati collegati globalmente in rete, la criminalità su Internet si è notevolmente diffusa. Eppure la piena dimensione della minaccia corrispondente non è ancora stata percepita; in parte essa si cela sempre dietro a un'immagine leggermente trasfigurata di un qualcosa di virtuale e di fittizio.

Il Consiglio federale svizzero ha riconosciuto l'importanza di questa problematica e ha dato seguito già due volte a una necessità molto ampia: una prima volta istituendo il Servizio di coordinazione nazionale per la lotta contro la criminalità su Internet (SCOCI)[1] e una seconda volta creando la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI)[2]. Sono così state istituite strutture adeguate ed efficienti per proteggere efficacemente la società dalle minacce menzionate qui sopra. Ciò che ancora mancava era una vasta analisi sullo stato della protezione e sulla situazione di minaccia nell'ottica dell'economia svizzera. In altri Paesi, primo fra tutti gli Stati Uniti, simili studi a livello nazionale sono disponibili da tempo nella forma dei CSI/FBI Computer Crime and Security Survey[3]. In questo senso il rapporto annuale 2005 presenta fatti ampiamente documentati. A titolo di esempio, si citi che la metà delle imprese USA interrogate è stata vittima di attacchi informatici nel corso dell'anno oppure che il 95 per cento di esse ha subito danni al proprio sito Web. Ancora più importante è la constatazione che tra il 2004 e il 2005 i costi per attacco informatico sono saliti repentinamente, segnatamente da una media di 51 000 dollari US a una media di circa 300 000 dollari US.

Questi dati non servono unicamente a sensibilizzare il pubblico. Essi consentono altresì alle imprese di effettuare confronti, di situare gli eventi subiti in un contesto più ampio, di meglio valutare l'efficienza delle misure adottate e infine di accertare la propria necessità di intervento. L'attuazione dello studio svizzero è stata affidata al Servizio di ricerca per la politica di sicurezza del PF di Zurigo[4].

I risultati confermano da un canto tendenze già note, ma sorprendono d'altro canto per fatti inaspettati. Gli esperti apprezzeranno indubbiamente questo rapporto: la sua facilità di comprensione lo renderà però anche interessante per tutti coloro che si occupano di sicurezza dell'informazione – una problematica a cui, alla lunga, non ci si potrà più sottrarre.

Mauro Vignati
Analista MELANI, Capoprogetto

1 http://www.scoci.ch.
2 http://www.melani.admin.ch.
3 Computer Security Institute(CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005).
4 http://www.css.ethz.ch.

Compendio dei principali risultati

Nel 2005 una chiara maggioranza delle imprese interrogate (72%) ha constatato almeno un evento concernente la sicurezza dell'informazione.
Gli eventi più diffusi sono i virus, i vermi informatici, i cavalli di Troia e lo spyware. Una minaccia constatata con relativa frequenza è il furto convenzionale di laptop o di altro hardware. Sono invece più rari gli attacchi mirati alla disponibilità dei mezzi informatici, l'hacking, il furto di dati o il deturpamento della homepage.

Le grandi imprese con oltre 250 collaboratori e le imprese che effettuano acquisti o vendite tramite Internet sono esposte a un maggiore rischio di eventi.
Gli attacchi mirati sono diretti con maggiore frequenza contro le grandi imprese e contro quelle che praticano l'e-Commerce.

Quasi tutte le imprese applicano misure tecniche e organizzative di protezione.
In ambito di misure tecniche quasi tutte le imprese utilizzano soprattutto i programmi antivirus e i firewall. A livello di misure organizzative la più diffusa è il backup-management. Misure tecniche e organizzative più dispendiose (p. es. organizzazioni di crisi) sono applicate precipuamente dalle grandi imprese e da quelle del settore informatico.

Le imprese dispongono di risorse finanziarie e di personale esigue per la sicurezza dell'informazione.
Soltanto in poche fra le imprese interrogate (32%) un informatico diplomato è responsabile della sicurezza dell'informazione.

Numerose imprese scorporano i loro rischi in ambito di sicurezza dell'informazione.
L'outsourcing è in particolare popolare presso le imprese medie. Sovente però i possibili danni dovuti a problemi in ambito di sicurezza dell'informazione sono assicurati.

Numerose imprese sarebbero favorevoli a una maggiore cooperazione.
La maggior parte di queste imprese ritiene che in vista della collaborazione debba essere istituita una nuova organizzazione. In caso di possibile cooperazione va però osservato che le esigenze delle diverse imprese sono molto differenziate.

1 Introduzione

Le tecnologie dell'informazione e della comunicazione (TIC) caratterizzano la vita quotidiana della maggior parte delle imprese e delle autorità svizzere. Esse consentono di lavorare in rete e semplificano la comunicazione. Con l'applicazione delle nuove tecnologie sono però apparsi anche nuovi problemi. Se negli anni Ottanta si dibatteva ancora dell'esistenza dei virus informatici, essi sono ora diffusi a livello mondiale e costituiscono soltanto una delle numerose possibili minacce alla sicurezza dell'informazione.

L'accresciuta dipendenza dalle tecnologie dell'informazione e della comunicazione nei più diversi settori di attività e la noncuranza talvolta osservata nella loro utilizzazione aumentano il pericolo di avarie TIC, che minacciano il funzionamento senza intoppi dei processi operativi dell'economia. Un blackout delle TIC costerebbe estremamente caro all'economia svizzera. Uno studio del Computer Engineering and Networks Laboratory (TIK) del PF di Zurigo ha accertato che in Svizzera il danno economico di un blackout di Internet durante una settimana si aggirerebbe sui 5,83 miliardi di franchi. Lo studio evidenzia la dipendenza dall'informatica e da Internet di una società moderna come la Confederazione. Il 48 per cento dei 3,6 milioni di posti di lavoro in Svizzera dipende dalle TIC[5].

In considerazione di questa situazione le imprese adottano misure diverse – a dipendenza delle esigenze di sicurezza e delle risorse disponibili. Si può trattare di misure tecniche che spaziano fino a misure organizzative o a una sensibilizzazione generale dei collaboratori.

L'obiettivo del presente studio è di realizzare un compendio delle minacce alle quali è esposta l'economia svizzera in ambito di sicurezza dell'informazione e di conoscere in che modo le imprese e le autorità le affrontano. Si tratta inoltre di analizzare se in tale ambito è possibile una cooperazione tra imprese e le modalità di protezione delle TIC delle imprese da parte dello Stato.

1.1 Metodo dello studio

Per fornire una panoramica possibilmente ampia, è stata effettuata un'inchiesta scritta presso le imprese e le autorità di tutte le categorie di dimensioni, di tutte le parti del Paese e di tutti i rami del secondario e del terziario (settore industriale e settore dei servizi). Complessivamente sono state contattate per lettera o per e-mail 4 916 imprese e autorità[6]. Nell'intento di ridurre al minimo il dispendio amministrativo, il questionario non è stato inviato fisicamente, ma è stato reso accessibile in Internet mediante il link protetto da password inviato ai partecipanti. Il questionario constava di 36 domande ed è stato messo a disposizione dei partecipanti allo studio per quattro settimane (15.03.2006–13.04.2006)[7]. Durante questo periodo di tempo sono stati compilati 562 questionari. La quota di riflusso è quindi dell'11,45 per cento e si situa pertanto nella media di simili inchieste[8].

5 Dübendorfer, Thomas, Arno Wagner e Bernhard Plattner, *An Economic Model for Large-Scale Internet Attacks* (Studi del Computer Engineering and Networks Laboratory del PF di Zurigo, 2004), pag. 4.
6 In merito alla scelta e alla composizione della verifica per campionatura cfr. l'allegato 1.
7 Il questionario e i dettagli del metodo di rilevamento figurano nell'allegato 5.
8 Per una valutazione dettagliata del riflusso cfr. l'allegato 2.

1.2 Stato della ricerca e studi comparati

La maggior parte degli studi esistenti nel settore della sicurezza delle TIC verte esclusivamente sugli aspetti tecnici o è concepita come raccomandazioni di intervento per i responsabili delle imprese. Non esistono inventari sulla sicurezza dell'informazione nelle imprese svizzere. È stata nondimeno di ausilio per il presente studio l'inchiesta «Impiego e sfruttamento di Internet nelle piccole e medie imprese della Svizzera» («Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz») realizzata nel 2002 dalla task force PMI[9], perché nell'analisi della sicurezza dell'informazione è importante sapere quale è la rilevanza dell'informatica nelle diverse imprese.

Negli altri Paesi sono in parte state effettuate ampie analisi della sicurezza dell'informazione nelle imprese. Per questo motivo i risultati vanno di volta in volta confrontati con gli studi internazionali. Costituiscono precipuamente importanti fonti di dati di raffronto lo «FBI Computer Crime Survey 2005»[10], lo studio «Hi-Tech Crime: The Impact on UK Business 2005» della National Hi-Tech Crime Unit britannica[11], nonché il rapporto «Die Lage der IT-Sicherheit in Deutschland 2005» del Bundesamt für Sicherheit in der Informatik (BSI) tedesco[12].

1.3 Terminologia

Questa sezione fornisce la definizione dei termini più frequentemente utilizzati nel presente studio.

Sicurezza dell'informazione
La sicurezza dell'informazione ha lo scopo di impedire la modifica o l'ottenimento non autorizzati di informazioni e di dati. La realizzazione di una sicurezza dell'informazione possibilmente elevata è garantita da un processo che, oltre a misure tecniche (di sistema), comprende anche misure aziendali e organizzative per la protezione delle informazioni.

Obiettivi di protezione nella sicurezza dell'informazione
Autenticità: per autenticità di un oggetto (p. es. dati, sistemi, server ecc.) o di un soggetto (utente, user) si intende la genuinità della loro identità, fermo restando che essa deve poter essere verificata sulla scorta di caratteristiche univoche.
Integrità dei dati: l'integrità dei dati è garantita se i soggetti e gli oggetti non possono modificare senza autorizzazione i dati da proteggere.
Confidenzialità: un sistema garantisce la confidenzialità se impedisce qualsiasi ottenimento non autorizzato di informazioni, anche durante il trasporto dei dati.
Disponibilità: un sistema è considerato disponibile se agli utenti autentificati e autorizzati non si può impedire di accedervi; per negare loro l'accesso è necessaria un'autorizzazione.

9 Sieber, Pascal, *Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (studio su mandato del Segretariato di Stato dell'economia, Berna, 2002).

10 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), 2005 Computer Crime and Security Survey (2005). http://www.gocsi.com.

11 National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005). http://www.gfknop.co.uk/content/news/news/Impact%20of%20HTC%20NOP%20Survey%202005.pdf

12 Bundesamt für Sicherheit in der Informationstechnik (BSI), *Die Lage der IT-Sicherheit in Deutschland 2005* (luglio 2005). http://www.bsi.bund.de/literat/lagebericht/lagebericht2005.pdf.

Vulnerabilità
Per vulnerabilità si intende un punto debole del sistema, che può pregiudicare gli obiettivi di protezione definiti qui sopra. La vulnerabilità può sussistere nei confronti di pericoli fisici (incendio, inondazione, terremoto, fulmine, panne di corrente), dell'uso inappropriato o ad esempio anche nei confronti del malware.

Minaccia
È data minaccia al sistema se sussistono una o più vulnerabilità che possono pregiudicare gli obiettivi di protezione definiti qui sopra.

Rischio
Il rischio designa la probabilità (o la frequenza relativa) che una minaccia produca un evento di danno nonché i costi consecutivi al danno. Il rischio dipende pertanto anche dall'entità dei valori da proteggere.

Attacco/evento
L'attacco designa un accesso non autorizzato o un tentativo di accesso a un sistema. Si opera una distinzione tra attacchi passivi (ottenimento non autorizzato di informazioni, perdita della confidenzialità) e attacchi attivi (modifica non autorizzata di dati, perdita dell'integrità o della disponibilità)[13].

Nondimeno, nel presente studio si parlerà di eventi perlopiù a titolo generale, per evidenziare che anche le manipolazioni errate senza cattive intenzioni possono sfociare in problemi di sicurezza dell'informazione.

13 Le definizioni sono riprese in modo semplificato e riassuntivo da: Eckert, Claudia, *IT-Sicherheit: Konzepte – Verfahren – Protokolle* (3a ed. rielaborata e ampliata, Monaco di Baviera, Oldenbourg, 2004), pagg. 4–17.

2 Frequenza degli eventi

In questa prima parte dell'analisi sono esaminati la frequenza degli eventi, la minaccia alla sicurezza dell'informazione da parte dei collaboratori delle imprese nonché il rischio di evento in funzione del tipo di impresa e della forma di minaccia. Anzitutto occorre però spiegare quali minacce alla sicurezza dell'informazione sono prese in considerazione e le modalità della loro definizione. Le spiegazioni relative alle singole minacce sono mantenute succinte perché informazioni più precise sono facilmente reperibili in Internet e nella letteratura[14].

2.1 Minacce alla sicurezza dell'informazione

Le imprese sono state interrogate sulle principali minacce per la sicurezza dell'informazione. Di massima possono essere minacciate la confidenzialità, la disponibilità e l'integrità dei dati. L'inchiesta non è stata estesa allo spam (detto anche junk e-mail), ossia all'invio indesiderato di pubblicità tramite e-mail. Questi e-mail possono invero essere sgradevoli, ma di norma non costituiscono una minaccia diretta alla sicurezza dell'informazione.

2.1.1 Descrizione delle minacce analizzate

Virus, spyware, vermi informatici e cavalli di Troia (malware generico)
Un *virus* consta di istruzioni di programma che impartiscono al computer le azioni da eseguire. Per propagarsi, il virus nidifica in un cosiddetto «programma ospite». Il «programma ospite» può essere un'applicazione (p. es. un software scaricato) o un documento (p. es. un file Word o un file Excel). Il virus viene attivato all'atto dell'esecuzione dell'applicazione o dell'apertura del documento. Di conseguenza il computer è indotto a eseguire le azioni nocive. Numerosi virus pervengono al computer tramite gli allegati di e-mail o file infettati scaricati da Internet. Ad avvenuta attivazione i virus possono anche spedirsi ulteriormente per e-mail avvalendosi dei contatti dell'elenco degli indirizzi. Altri percorsi di propagazione sono costituiti dai supporti esterni di dati (p. es. CD-ROM, USB Memory Stick ecc.).

Lo *spyware* è destinato a raccogliere informazioni all'insaputa dell'utente e a trasmetterle a un indirizzo predefinito. Le informazioni da selezionare dipendono dal singolo spyware e spaziano dalle abitudini di navigazione in Internet ai parametri di sistema, alle password e ai documenti confidenziali.

Come i virus, i *vermi informatici* constano di istruzioni di programma che stabiliscono le azioni che devono essere effettuate dal computer. Diversamente dai virus essi non necessitano di un programma ospite per propagarsi. Essi sfruttano piuttosto le lacune di sicurezza o gli errori di configurazione del sistema operativo per propagarsi autonomamente da un computer all'altro. Un obiettivo possibile dei vermi informatici sono i computer che presentano lacune di sicurezza o errori di configurazione e sono collegati in qualsiasi forma ad altri computer (p. es. tramite Internet, una rete locale ecc.).

I *cavalli di Troia* (denominati frequentemente troiani) sono programmi che eseguono di nascosto azioni nocive, camuffandosi agli occhi dell'utente da applicazioni e file utili. Sovente i

14 Informazioni su: http://www.melani.admin.ch/gefahren-schutz/gefahren/index.html?lang=de. La letteratura comprende numerose opere di compendio sulla sicurezza dell'informazione. Informazioni dettagliate in merito in: Bidgoli, Hossein et al. (ed.), *Handbook of Information Security Volume 3* (Hoboken, 2006).

cavalli di Troia sono programmi scaricati da Internet. Si può però anche trattare di brani musicali o di filmati. Essi sfruttano le lacune di sicurezza dei singoli programmi di riproduzione (p. es. Media Player) per installarsi inosservatamente nel sistema. Spesse volte essi sono pure propagati tramite gli allegati degli e-mail. Nella maggior parte dei casi essi sono destinati allo spionaggio di dati confidenziali, al controllo integrale del computer o all'invio di spam tramite il computer infettato.

Attacchi alla disponibilità (Denial of Service, DoS)

Gli attacchi alla disponibilità hanno l'obiettivo di impedire all'utente l'accesso a un determinato servizio o perlomeno di renderlo molto difficile. Una variante popolare degli attacchi DoS in ambito di TI è l'invio di numerosissime richieste a un computer/servizio. Il grande numero di richieste sovraccarica a tal punto il computer/servizio da rallentare notevolmente i tempi di risposta o da metterlo totalmente fuori uso.

Gli attacchi provengono sovente da più computer manipolati in precedenza con malware. Si parla in questo caso di attacchi di Distributed (ripartito) Denial of Service (DDoS). Tali attacchi sono soprattutto efficaci contro le imprese che intendono disbrigare affari tramite Internet. Essi sono sovente abbinati a ricatti.

La minaccia di attacchi DDoS è anche in aumento perché numerosi computer sono infettati all'insaputa da malware e possono quindi essere manipolati abusivamente da hacker. È segnatamente possibile eseguire facilmente attacchi DDoS se più computer manipolati sono integrati in una rete (cosiddetta rete bot). Gli esperti mettono pertanto in guardia da un possibile aumento di questi attacchi.

Penetrazione nel sistema (hacking) e furto di dati

La nozione di hacking non corrisponde a una definizione esatta. Essa è sovente utilizzata per tutti i tipi di manipolazione su computer di terzi. Nella presente fattispecie lo hacking designa la penetrazione non autorizzata nel sistema informatico di un'impresa. Tale penetrazione è spesso realizzata tramite l'impiego mirato di programmi di spionaggio (spyware, cavalli di Troia). Gli hacker possono leggere, modificare o cancellare i dati dei sistemi nei quali sono penetrati. I danni maggiori sono provocati da hacker mossi da intenti criminali che rubano i dati di un'impresa. L'obiettivo di simili attacchi sono sovente i dati confidenziali sulla clientela o nuovi sviluppi di idee dai quali dipende la sopravvivenza economica dell'impresa. Il furto di dati può pertanto avere gravissime conseguenze per un'impresa. Di solito, questo tipo di attacchi è difficilmente individuabile.

Deturpamento della homepage (defacement)

Il deturpamento di una o più homepage (mass defacement) è effettuato avvalendosi delle lacune di sicurezza dei server Web. Gli aggressori modificano successivamente il contenuto e il design delle homepage. Talvolta questi attacchi sono motivati politicamente e sono perpetrati da cosiddetti «hacktivisti» per dare visibilità a una protesta politica. Altre volte invece le homepage sono deturpate per divertimento da «script-kiddies». A seconda dell'importanza della homepage per l'attività commerciale dell'impresa, le ripercussioni di simili attacchi spaziano dal danno all'immagine a ingenti perdite finanziarie.

Abuso delle reti wireless

I Wireless Local Area Networks (WLAN) offrono un accesso senza fili e complicazioni a Internet. Tramite questi accessi insufficientemente protetti, gli aggressori possono utilizzare abusivamente il collegamento per molteplici scopi. È soprattutto problematico il fatto che l'uso abusivo delle reti wireless venga individuato troppo tardi o non venga affatto scoperto.

Furto convenzionale di laptop e di altro materiale informatico
Nonostante tutte le nuove forme di minaccia, non va scordato che il materiale informatico può essere rubato anche in maniera convenzionale. In caso di furto, oltre alla perdita del valore materiale, possono verificarsi altri ingenti danni se sul laptop sottratto sono ad esempio stati memorizzati dati sensibili.

2.1.2 Frequenza degli eventi

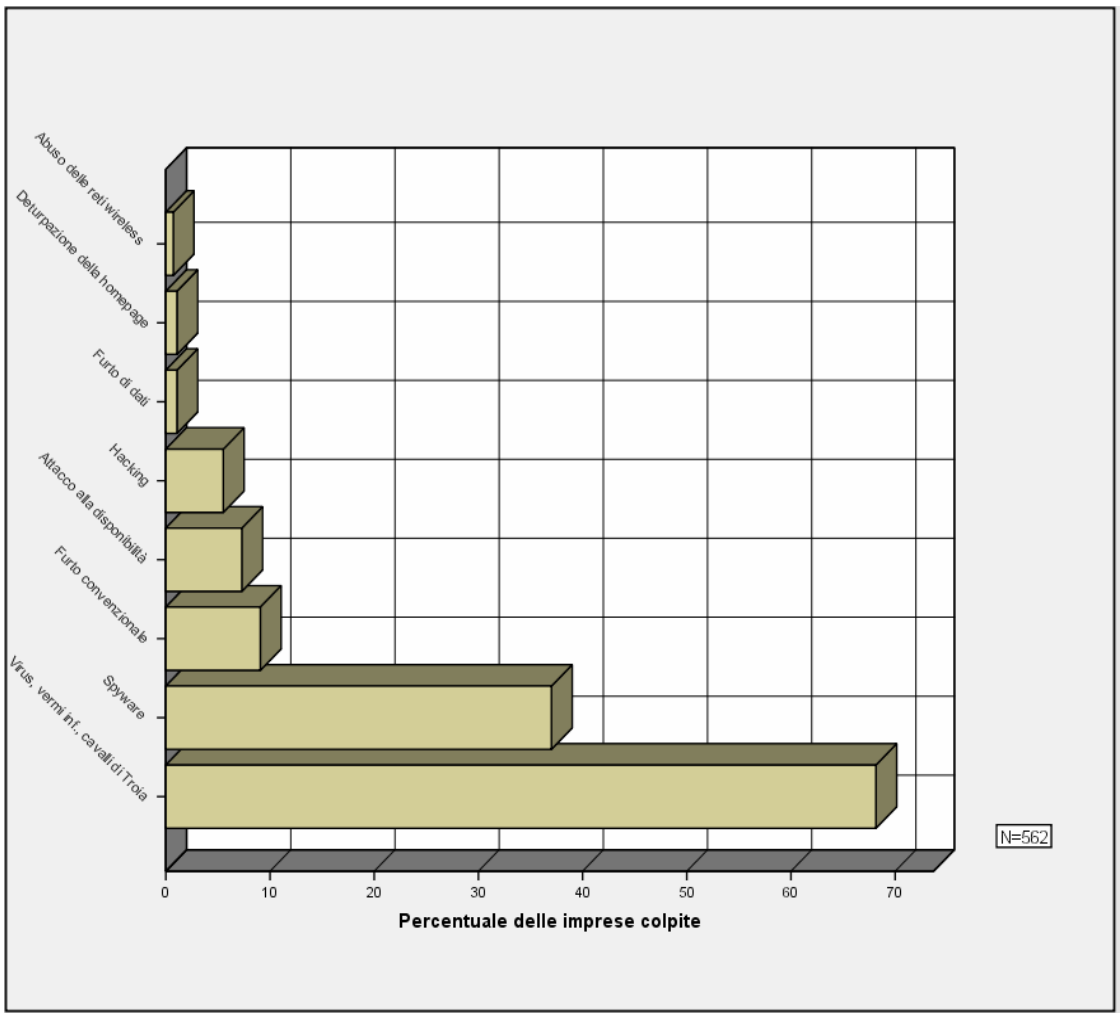
Nel quadro dell'inchiesta si è indagato se nel 2005 le imprese sono state toccate dalle minacce descritte qui sopra. Dallo spoglio emerge che gli eventi concernenti la sicurezza dell'informazione si verificano frequentemente. Il 72 per cento delle imprese che hanno partecipato all'inchiesta ammette che almeno una delle minacce tratteggiate qui sopra ha determinato un evento concernente la loro struttura di informazione. Va però osservato che i partecipanti all'inchiesta non costituiscono una riproduzione proporzionale della realtà. A titolo di esempio il 15 per cento dei partecipanti all'inchiesta sono grandi imprese con oltre 250 collaboratori, mentre in realtà soltanto lo 0,4 per cento di tutte le imprese raggiunge simili dimensioni. Inoltre, nell'ambito delle imprese interrogate alcuni settori sono più rappresentati che non nella realtà[15]. A causa di questa composizione non proporzionale delle imprese interrogate, dalle affermazioni della media dei partecipanti all'inchiesta non si può direttamente desumere la media di tutte le imprese svizzere del secondario e del terziario. Tuttavia, poiché si devono effettuare stime sulla frequenza reale degli eventi, si applica la procedura statistica della ponderazione. In tale contesto la realtà è simulata valutando in maniera diversa le indicazioni delle imprese[16]. Se si applica questa procedura, la percentuale di imprese svizzere che nel 2005 ha individuato almeno uno degli eventi descritti può essere stimata al 63 per cento.

In considerazione del fatto che le diverse minacce possono avere ripercussioni diverse, è importate conoscere la frequenza dei singoli eventi. La figura 1 mostra quali eventi hanno toccato quante imprese e autorità.

15 Sul riflusso per categorie di dimensioni e settori cfr. l'allegato 2.

16 Tutti i dati sono moltiplicati per un fattore di ponderazione. Per maggiori informazioni sulla procedura di ponderazione cfr. l'allegato 3.

Figura 1 Frequenza degli eventi



È chiaro che il malware (virus, vermi informatici, cavalli di Troia e spyware) è il più diffuso. Al terzo posto della graduatoria figura il furto convenzionale di materiale informatico. Gli attacchi tecnicamente più dispendiosi, ma gravi quanto alle loro ripercussioni, sono individuati molto meno sovente.

2.1.3 La minaccia da parte dei propri collaboratori

Le conoscenze sulla frequenza degli eventi permettono di valutare meglio il rischio delle imprese. In questo contesto è importante conoscere l'origine degli eventi. È particolarmente interessante sapere di quanti eventi sono responsabili i propri collaboratori.

I collaboratori possono mettere in pericolo la sicurezza dell'informazione delle loro imprese per diversi motivi. Da un canto è sovente il loro comportamento illecito a rendere primariamente possibile l'introduzione di malware o la perpetrazione di attacchi mirati; d'altro canto i collaboratori stessi possono essere gli autori di un attacco – ad esempio a scopo di arricchimento o per motivi di vendetta nei confronti dei loro superiori. Numerosi esperti ritengono che i

collaboratori sono direttamente responsabili di una percentuale elevata di eventi[17]. Anche dallo studio britannico «Hi-Tech Crime: The Impact on UK Business 2005» risulta una percentuale elevata di autori all'interno delle imprese. Secondo questo studio il 37 per cento degli eventi registrati nelle imprese britanniche possono essere ricondotti a manipolazioni intenzionali da parte di collaboratori disonesti o insoddisfatti[18]. Nel nostro studio questo si verifica soltanto per il 10 per cento delle imprese interrogate, un tasso nettamente inferiore alle previsioni. Non è tuttavia possibile un confronto diretto con lo studio britannico perché nel suo contesto sono state in parte analizzate ulteriori minacce e perché vi hanno partecipato unicamente imprese con oltre 100 collaboratori.

Si può comunque constatare che gli eventi direttamente riconducibili a un collaboratore sono piuttosto rari in Svizzera. Solo in casi eccezionali i collaboratori di un'impresa le arrecano intenzionalmente danni. La minaccia alla sicurezza dell'informazione dovuta a comportamenti illeciti non intenzionali dovrebbe essere molto più elevata.

2.1.4 La frequenza degli eventi nel raffronto internazionale

Come vanno ora valutate le frequenze rilevate di eventi nel confronto con gli studi internazionali? Nel quadro dell'ampia inchiesta «Computer Crime Survey 2005» dell'FBI, l' 87 per cento dei partecipanti ammette di avere constatato un evento. In questo contesto sono però state prese in considerazione unicamente imprese con più di cinque posti a tempo pieno. Ai fini del confronto devono dunque essere scorporate le imprese con meno di cinque collaboratori. Il 79 per cento di tutte le imprese e autorità svizzere con più di cinque collaboratori ha constatato un evento. La percentuale è leggermente inferiore a quella dello studio dell'FBI, poiché in quest'ultimo gli eventi sono stati definiti in modo un po' più completo. Lo studio dell'FBI enumera infatti come evento anche la scoperta di materiale pornografico.

Anche il già citato studio britannico «Hi-Tech Crime: The Impact on UK Business 2005» evidenzia che in materia di sicurezza dell'informazione la Svizzera ha problemi analoghi a quelli degli altri Paesi. Nel quadro dell'inchiesta, condotta su grandi imprese con oltre 100 collaboratori, è risultato che l'89 per cento di esse ha constatato un evento nel 2004. Se si considerassero unicamente le imprese con oltre 100 collaboratori, anche in Svizzera ne sarebbe interessato l'85 per cento.

Anche per quanto concerne i tipi di eventi i risultati corrispondono all'incirca a quelli degli studi internazionali. Lo studio dell'FBI ha altresì evidenziato che i virus e lo spyware sono di gran lunga il problema più frequente, mentre il furto convenzionale si verifica abbastanza sovente e gli attacchi mirati sono piuttosto rari.

Si può quindi affermare che le imprese svizzere non constatano né più né meno eventi di quelle degli altri Paesi. A causa del carattere globale della messa in rete, le minacce alla sicurezza dell'informazione concernono in uguale misure le imprese di tutti i Paesi.

17 In un rapporto della ditta Gartner si parte addirittura dal presupposto che il 70% degli abusi dell'informatica siano opera dei collaboratori. Gartner Research, *Enterprises and Employees: The Growth of Distrust* (2005). Compendio dei risultati in: http://www.csoonline.com/analyst/report3317.html. Anche il Bundesamt für Sicherheit in der Informationstechnik tedesco parte dall'idea di una percentuale elevata di autori all'interno dell'impresa: Bundesamt für IT-Sicherheit, *Die Lage der IT-Sicherheit in Deutschland 2005* (luglio 2005), pag. 29.

18 The National Hi-Tech Crime Unit (nhctu), *Hi-Tech Crime, The Impact on UK Business 2005* (2005), pag. 20.

2.2 Il rischio di un evento secondo il tipo di impresa

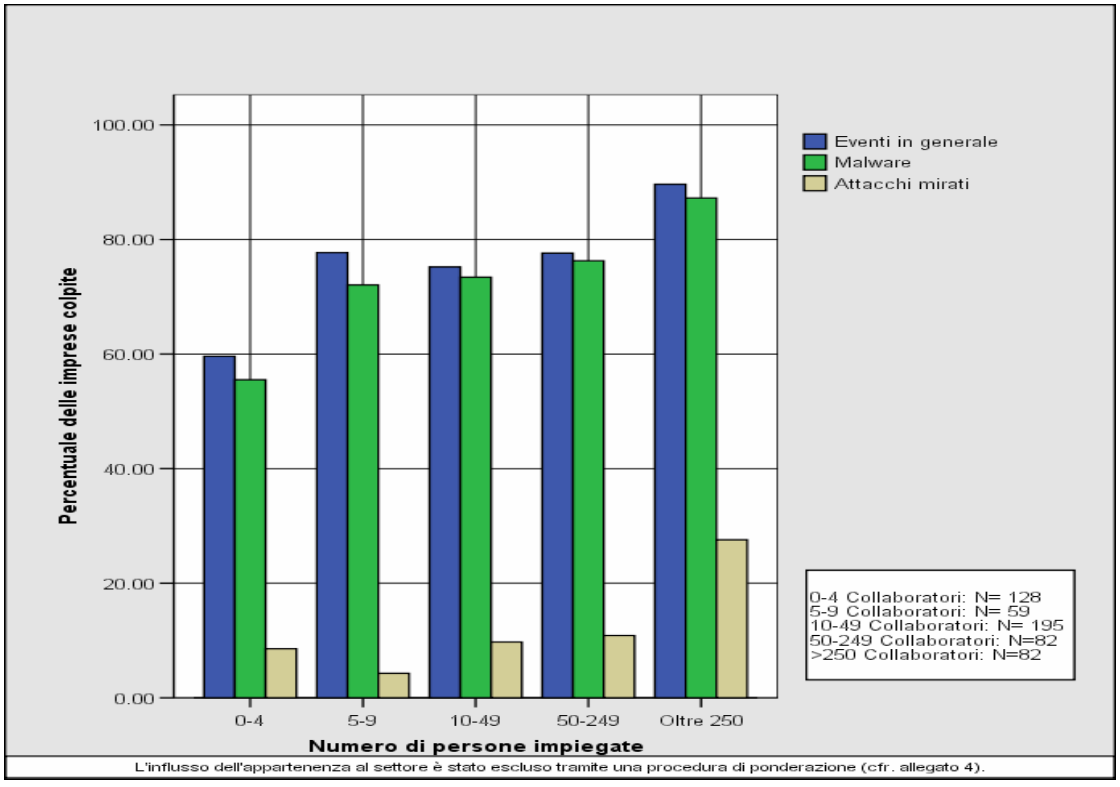
Se la nazionalità di un'impresa non esercita alcun influsso sul rischio di evento, si può invece presupporre che le dimensioni e il campo di attività di un'impresa influenzino la probabilità di malware e di attacchi mirati. Qui di seguito si analizzerà quali tipi di imprese sono esposti con particolare frequenza agli eventi.

2.2.1 Il rischio in funzione delle dimensioni dell'impresa

Nello studio della task force sulla diffusione dell'informatica e di Internet nelle imprese è stato comprovato che esiste un nesso tra le dimensioni dell'impresa e l'impiego dell'informatica. Quanto più grande à l'impresa, tanto più importanti divengono le tecnologie informatiche e di Internet[19]. Il rischio di eventi cresce però parallelamente all'utilizzazione più intensiva di questi mezzi. A titolo di esempio, quanti più collaboratori ricevono e inviano e-mail, tanto maggiore è la probabilità che possano infiltrarsi virus nella rete aziendale. Inoltre le imprese di maggiori dimensioni sono più attrattive per gli attacchi mirati. Il dispendio necessario a un solo attacco mirato è proficuo per l'hacker soltanto se l'impresa oggetto dell'attacco realizza una cifra d'affari sufficiente o dispone di valori patrimoniali sufficientemente importanti da poter essere intaccati o sottratti in un modo o nell'altro. Nelle imprese di maggiori dimensioni c'è ovviamente più denaro da sottrarre che in quelle di dimensioni minori.

La figura 2 illustra come la probabilità di un evento aumenta in funzione delle dimensioni delle imprese.

Figura 2 Rischio di eventi per categorie di dimensioni



19 Sieber, Pascal, *Einsatz und Nutzung des Internets in den kleinen und mittleren Unternehmen in der Schweiz. Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Berna 2002), pag. 19.

Risulta chiaramente che le microimprese, ossia quelle con meno di cinque collaboratori, hanno constatato complessivamente il minor numero di eventi. Le piccole e medie imprese (5–9, 10–49 e 50–249 collaboratori) costituiscono un gruppo particolarmente omogeneo. Esse incontrano invero maggiori problemi con il malware, ma non riscontrano un numero più significativo di attacchi mirati rispetto alle imprese più piccole. Gli attacchi mirati concernono prevalentemente le grandi imprese con oltre 250 collaboratori. Il 28 per cento di queste imprese ha rilevato un attacco del genere. Anche il malware concerne con maggiore frequenza le grandi imprese piuttosto che le piccole e medie imprese.

In questo senso i risultati corrispondono all'incirca alle aspettative. La differenza tra microimprese e grandi imprese è molto evidente. Un po' sorprendente è forse il fatto che non esistano praticamente differenze tra le piccole imprese con 5–9 collaboratori e le medie imprese che contano fino a 249 collaboratori.

2.2.3 Il rischio in funzione dell'attività commerciale

Per differenziare le imprese in funzione della loro attività ci si fonda solitamente sulla loro appartenenza a un settore[20]. Si presuppone che le imprese del medesimo settore disbrighino in maniera analoga i loro affari. Anche nell'ambito del presente studio saranno esaminati i diversi rischi dei settori.

Come la dimensione delle imprese anche l'appartenenza a un settore esercita un influsso sull'importanza delle tecnologie dell'informatica e di Internet nelle imprese[21]. Bisogna altresì presumere che non tutti i settori siano esposti al medesimo rischio di attacco mirato perché tali attacchi sono piuttosto attesi nei settori nei quali vengono realizzate ingenti cifre d'affari oppure in settori che dispongono di valori patrimoniali che possono essere intaccati tramite attacchi perpetrati con l'ausilio delle TIC. A titolo di esempio, si ipotizza quindi che le imprese del settore finanziario e del settore informatico – che sfruttano intensamente l'informatica e generano cifre d'affari elevate – constatino eventi con maggiore frequenza rispetto alle imprese del settore edilizio e del settore della ristorazione.

La valutazione dei risultati dell'inchiesta non conferma però questa ipotesi. Le imprese del settore dell'informatica registrano invero una grande frequenza di eventi, ma nel contempo le imprese del settore finanziario registrano un numero di eventi basso quanto quello registrato dalle imprese del settore della ristorazione[22]. È possibile che i risultati non corrispondano alle aspettative perché i singoli settori si proteggono bene, seppure in maniera diversa[23].

È però probabile che nemmeno la differenziazione in funzione dei settori sia particolarmente adeguata per desumere un rischio di evento dall'attività commerciale. Le tecnologie informatiche e di Internet possono svolgere un ruolo molto diverso all'interno dei settori. Un criterio adeguato

20 Si opera una differenziazione tra 12 diversi settori. Per i dettagli della suddivisione in settori cfr. l'allegato 1.

21 I risultati dell'inchiesta corrispondono in merito ai risultati dello studio della task force PMI. Sieber, Pascal, *Einsatz und Nutzung des Internets in den kleinen und mittleren Unternehmen in der Schweiz. Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Berna, 2002), pag. 20.

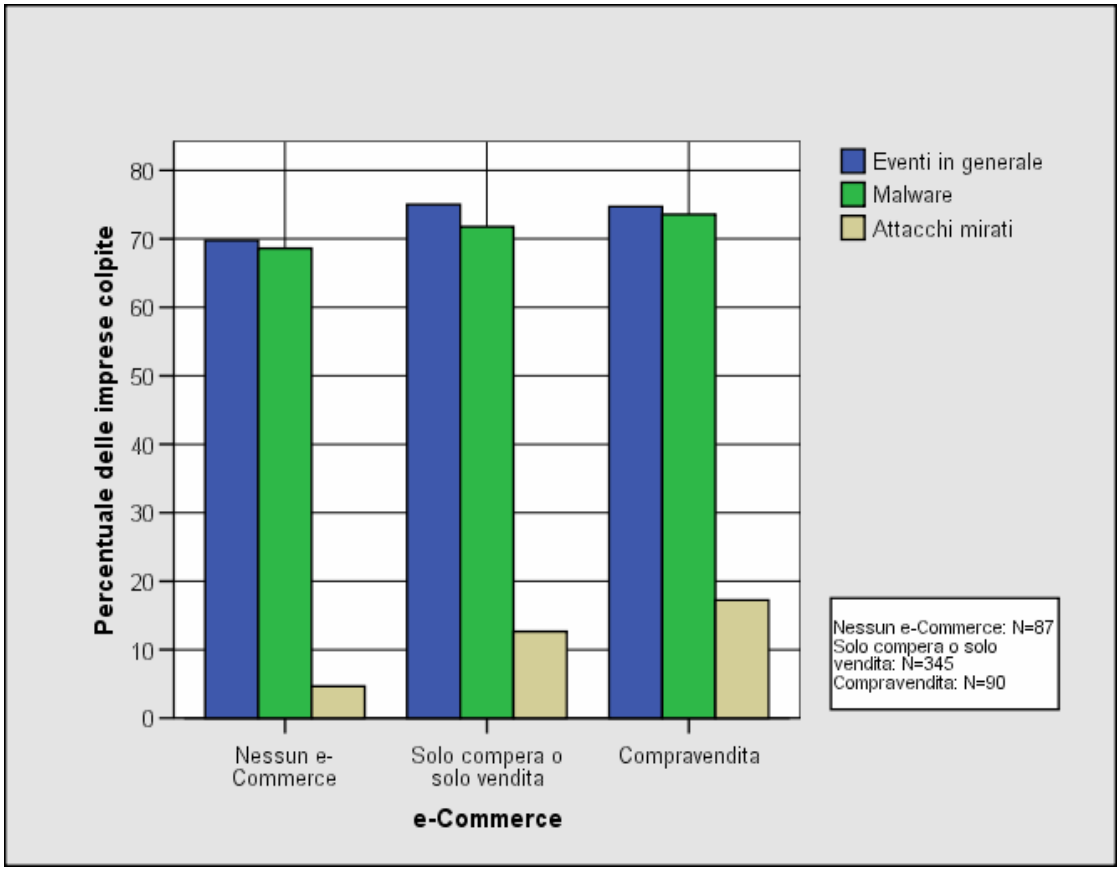
22 Se i risultati sono ponderati in funzione delle dimensioni delle imprese risulta che il 71% delle imprese del settore finanziario e il 73% delle imprese del settore della ristorazione hanno constatato un evento. La percentuale più elevata di imprese che hanno constatato un evento è quella registrata presso le aziende che forniscono servizi alle imprese (86%), mentre la percentuale minore è quella registrata presso le imprese del settore del commercio (61%).

23 Il tema del management dei rischi sarà trattato dettagliatamente nel prossimo capitolo.

di attività commerciale che potrebbe influire sul rischio deve pertanto evidenziare un nesso più forte con l'utilizzazione delle tecnologie informatiche e di Internet. Un simile criterio è costituito dagli acquisti e dalle vendite in Internet.

Per le imprese svizzere il cosiddetto e-Commerce è divenuto molto importante. Il 77 per cento delle imprese interrogate acquista prodotti o prestazioni di servizi tramite Internet.[24] Una percentuale sensibilmente minore di imprese, ossia il 19 per cento, vende prodotti o prestazioni di servizi tramite la propria homepage[25]. Si può supporre che constatino eventi soprattutto le imprese che esercitano l'e-Commerce; per questa ragione ci si aspetta perlopiù un aumento di attacchi mirati.

Figura 3 Rischio di eventi tramite e-Commerce in funzione dell'attività commerciale



La figura 3 conferma questa ipotesi. Le imprese che esercitano l'e-Commerce sono esposte a un rischio chiaramente maggiore di attacco mirato. Il 12 per cento delle imprese che effettuano acquisti o vendite tramite Internet e addirittura il 17 per cento di quelle che praticano sia gli acquisti sia le vendite hanno constatato un attacco mirato. Simultaneamente la frequenza di malware generico non utilizzato in maniera mirata aumenta solo debolmente. Le imprese che non

24 Conformemente alla ponderazione statistica (cfr. allegato 3) si tratta pur sempre del 73%. Questa percentuale molto elevata corrisponde agli studi precedenti in ambito di e-Commerce. Il rapporto di rete 2 (2001) indicava che il 60% delle imprese effettua acquisti tramite Internet. Lo studio della task force PMI rilevava invece per le PMI un tasso del 29% soltanto. Indicazioni tratte da: Sieber, Pascal, *Einsatz und Nutzung des Internets in den kleinen und mittleren Unternehmen in der Schweiz. Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Berna, 2002), pag. 32.

25 Si tratta del 14% se la percentuale di tutte le imprese svizzere è stimata applicando la procedura di ponderazione (cfr. allegato 3).

praticano l'e-Commerce registrano invero un numero pressoché uguale di eventi, ma essi sono raramente costituti da attacchi mirati (solo il 5% di queste imprese ha constatato un attacco).

Corrisponde quindi al vero l'ipotesi dell'aumento di attacchi mirati nei confronti delle imprese che praticano l'e-Commerce. Per valutare il rischio di malware generico non è invece rilevante se l'impresa svolga o meno affari tramite Internet. In considerazione del fatto che i virus, i vermi informatici, i cavali di Troia e lo spyware non programmati per un impiego specifico e individualizzato sono di per sé propagati in maniera più ampia – senza essere prevalentemente diretti nei confronti delle attività commerciali delle imprese –, il rischio di malware è altrettanto probabile presso le imprese che non si avvalgono di Internet per il disbrigo dei loro affari.

2.2.3 Conclusione e altri eventuali influssi sul rischio

Si constata che determinate imprese sono maggiormente esposte rispetto ad altre al rischio di eventi concernenti la sicurezza dell'informazione. Le dimensioni dell'impresa e l'utilizzazione di Internet per il disbrigo degli affari rivestono un ruolo importante.

Oltre alle dimensioni dell'impresa e alla sua attività commerciale, altri fattori possono influenzare il rischio di un evento, come il tipo di collegamento a Internet, il grado di innovazione tecnica o la rinomanza dell'impresa. Sarebbe quindi necessaria un'analisi più approfondita per potere predire la messa in pericolo della sicurezza dell'informazione per le singole imprese.

Ci si può chiedere se ciò sia possibile. Nell'analisi dei rischi in funzione del tipo di impresa non bisogna infatti dimenticare che le imprese hanno potuto indicare unicamente gli eventi scoperti. Ma nel caso appunto degli attacchi mirati accade sovente che essi rimangano ignoti per lungo tempo.

Va inoltre osservato che le imprese reagiscono in modo diverso alle minacce alla sicurezza dell'informazione. Le misure tecniche e organizzative di protezione possono ridurre la probabilità di un evento respingendo precocemente la minaccia, rispettivamente riducendo le vulnerabilità esistenti, in modo che il rischio diminuisca nonostante il carattere identico della minaccia. Simultaneamente il miglioramento delle misure di protezione fa sì che nelle imprese gli eventi siano scoperti anzitempo. Pertanto il capitolo successivo esamina in maniera più approfondita il management dei rischi nelle imprese.

3 Management dei rischi

Per quanto molteplici siano le minacce alla sicurezza dell'informazione, altrettanto vasto è il campo delle possibili contromisure. Il management dei rischi consta di misure tecniche, ma abborda altresì questioni strategiche e organizzative. Per non perdere la visione d'insieme, i diversi aspetti parziali del management dei rischi sono analizzati separatamente nel contesto del presente capitolo.

L'analisi verte anzitutto sulle misure tecniche e organizzative e sulla loro diffusione in seno alle imprese. Successivamente viene esaminata la questione delle risorse finanziarie e di personale utilizzate dalle imprese per il management dei rischi in ambito di sicurezza dell'informazione. È interessante analizzare se vi sono differenze significative tra le diverse imprese proprio perché esse, solitamente, sono disposte a investire soltanto il minimo indispensabile nella sicurezza dell'informazione. L'ultima sezione, infine, analizza con quale frequenza le imprese svizzere delegano il compito della sicurezza dell'informazione a esperti esterni e se esse tentano di coprire i rischi tramite un'assicurazione.

3.1 Misure tecniche e organizzative di protezione

Ai fini del management dei loro rischi è decisivo che le imprese adottino le misure ad esse meglio adeguate. Il presente capitolo analizza quale delle diverse possibilità è maggiormente utilizzata da quali imprese. Per garantire una visione d'insieme in questo contesto si opera una distinzione tra misure tecniche e misure organizzative.

3.1.1 Definizione delle misure tecniche

Prima di poter discutere in merito alla diffusione delle misure, occorre fornirne una definizione succinta, fermo restando che per una descrizione più dettagliata si rinvia nuovamente alle informazioni in Internet e alla letteratura[26].

Programmi antivirus
I programmi antivirus fanno parte della dotazione di base delle misure tecniche per la protezione della sicurezza dell'informazione. Questi programmi rintracciano il malware che si è annidato nel computer e lo bloccano o l'eliminano. A tale scopo è indispensabile conoscere i modelli di malware. Poiché sono in continua apparizione nuovi virus e vermi informatici, è necessario aggiornare costantemente i programmi antivirus.

Firewall
L'obiettivo di un firewall è proteggere i sistemi di computer da intrusi indesiderati e dalle minacce di malware. A tale scopo i firewall sorvegliano i collegamenti entranti e uscenti. Nelle imprese i firewall vengono solitamente impiegati sulle interfacce tra Internet e la propria rete; anche i firewall fanno parte delle misure tecniche standard.

26 http://www.melani.admin.ch/gefahren-schutz/gefahren/index.html?lang=de. Le misure sono descritte in maniera particolareggiata in: Bidgoli, Hossein et al. (ed.) *Handbook of Information Security Volume 3* (Hoboken, 2006).

Encryption (cifratura)
Poiché sulle reti di computer sono memorizzate informazioni delicate, sussiste sempre il rischio che persone non autorizzate pervengano alle informazioni. Il medesimo pericolo sussiste nella comunicazione di dati confidenziali (p. es. tramite e-mail). Per questo motivo si utilizzano programmi di cifratura. Nel loro contesto i dati sono convertiti in un «testo segreto» tramite un'apposita procedura di cifratura (algoritmo) e possono essere decrittati unicamente da chi dispone della chiave corrispondente. Per l'utente ciò significa un maggiore dispendio che si giustifica se la segretezza dell'informazione è di importanza centrale.

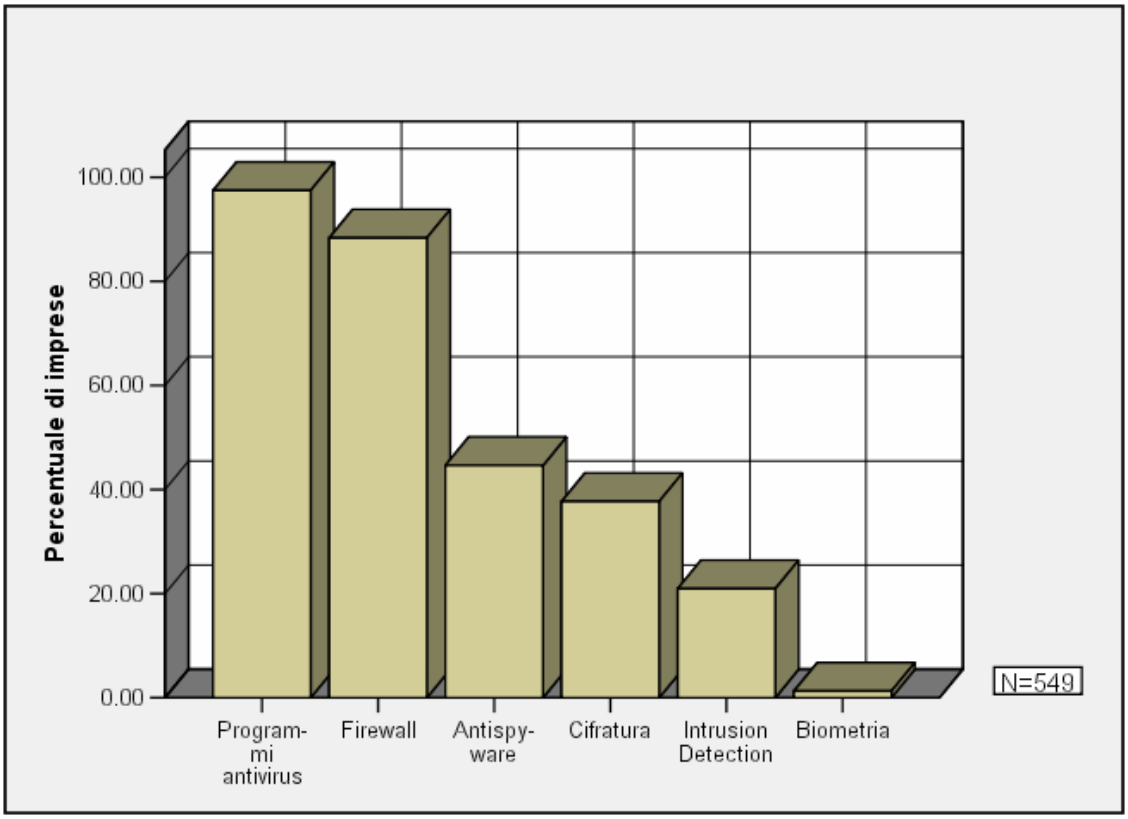
Intrusion Detection (individuazione degli attacchi)
Un Intrusion Detection System (IDS) è un programma che sorveglia, memorizza e analizza le attività su un computer o su una rete. Il sistema dà l'allarme non appena viene registrata un'attività corrispondente a un modello tipico di attacco. L'utilizzazione sensata di un IDS presuppone però conoscenze più approfondite di quelle necessarie ai firewall e ai programmi antivirus.

Misure biometriche
Queste misure possono essere utilizzate per limitare l'accesso fisico ai computer. L'utente deve ad esempio identificarsi tramite impronte digitali, riconoscimento del volto e caratteristiche degli occhi. La maggior parte delle procedure è relativamente dispendiosa.

3.1.2 L'applicazione di misure tecniche

La figura 4 illustra la diffusione tra le imprese svizzere delle misure descritte qui sopra.

Figura 4 Applicazione di misure tecniche di protezione



Nel complesso quasi tutti i partecipanti, ossia il 99,6 per cento, si protegge con almeno una delle misure tecniche. I programmi antivirus e i firewall sono utilizzati da oltre l'80 per cento delle imprese.

Se quindi la maggior parte delle imprese ha adottato le misure tecniche elementari di sicurezza, le tecnologie più dispendiose come ad esempio l'Intrusion Detection e la biometria sono sfruttate più raramente. Questo risultato sorprende poco e corrisponde grosso modo ai risultati forniti dai rilevamenti effettuati dal CSI e dall'FBI presso le imprese statunitensi[27]. È comprensibile che per motivi di costi le imprese utilizzino raramente queste misure tecnicamente e finanziariamente più dispendiose. Per alcune imprese tali misure non sono neppure sensate. Vale quindi la pena esaminare più attentamente quali imprese utilizzano le misure più dispendiose.

Si constata che queste misure sono adottate precipuamente dalle grandi imprese. A titolo di esempio, il 60 per cento delle grandi imprese applica tecniche di cifratura, mentre soltanto il 25 per cento delle microimprese ne fa uso. Dal confronto fra i diversi settori emerge che sono le imprese del settore informatico e del settore finanziario a fare più largo uso di misure tecniche dispendiose[28]. Questi risultati erano scontati perché le imprese maggiori e specialmente quelle del settore finanziario dipendono fortemente da un'infrastruttura informatica sicura. Considerata la presenza di un vasto know-how, non sorprende neppure la più ampia diffusione di misure tecniche dispendiose presso le imprese del settore informatico.

3.1.3 Definizione delle misure organizzative

Le imprese possono potenziare la sicurezza dell'informazione applicando diverse misure organizzative, oltre alle misure tecniche. Nel quadro dell'inchiesta esse sono state interrogate in merito alle principali misure di questo genere. Ne diamo qui sotto una descrizione succinta.

Security Policy
La Security Policy di un'impresa costituisce il concetto di base della sicurezza dell'informazione. In essa sono stabiliti gli obiettivi conformemente alle esigenze di sicurezza dell'impresa e definiti i mezzi a disposizione. Questi concetti devono essere chiari, affinché le diverse unità di un'impresa collaborino senza intoppi nell'ambito della sicurezza dell'informazione.

Management degli eventi (Incident Response)
Nel caso del management degli eventi si tratta di prepararsi a un possibile attacco nei confronti della sicurezza dell'informazione. A tale scopo dovrebbero essere prese in considerazione sia misure organizzative, sia misure legali. L'obiettivo di un simile management è di ristabilire nella maniera più rapida possibile la prontezza di impiego dell'informatica dopo un evento.

Management della salvaguardia dei dati (backup)
La salvaguardia dei dati serve alla protezione contro qualsiasi genere di perdita di dati. A tale scopo viene creata una copia dei dati (backup) che è conservata in un posto sicuro. In ambito di elaborazione di un management della salvaguardia dei dati bisogna soprattutto chiarire le

27 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005), pag. 5.

28 Il 63% delle imprese del settore finanziario utilizza tecnologie di cifratura, il 42% l'Intrusion Detection e il 5% misure biometriche. Nel caso delle imprese del settore informatico, il 57% utilizza tecnologie di cifratura, il 41% l'Intrusion Detection e il 5% misure biometriche. In questo senso queste imprese sono chiaramente all'avanguardia nell'applicazione di tecnologie dispendiose.

questioni della frequenza di salvaguardia, del responsabile della salvaguardia, dei dati da salvaguardare (tutti, soltanto i più importanti, soltanto i più recenti) e della modalità di gestione dei dati del backup.

Attualizzazione e colmatura delle lacune di sicurezza (Updates / Vulnerability Scan)
La grande complessità dei sistemi operativi e delle possibili applicazioni ha per conseguenza la scoperta di sempre nuove lacune di sicurezza, successivamente sfruttate dagli hacker o dal malware. È quindi di importanza decisiva potere individuare precocemente le lacune di sicurezza e colmarle tramite cosiddetti patch. Decisiva è anche una chiara ripartizione delle responsabilità di management degli aggiornamenti, affinché questi ultimi possano essere effettuati regolarmente.

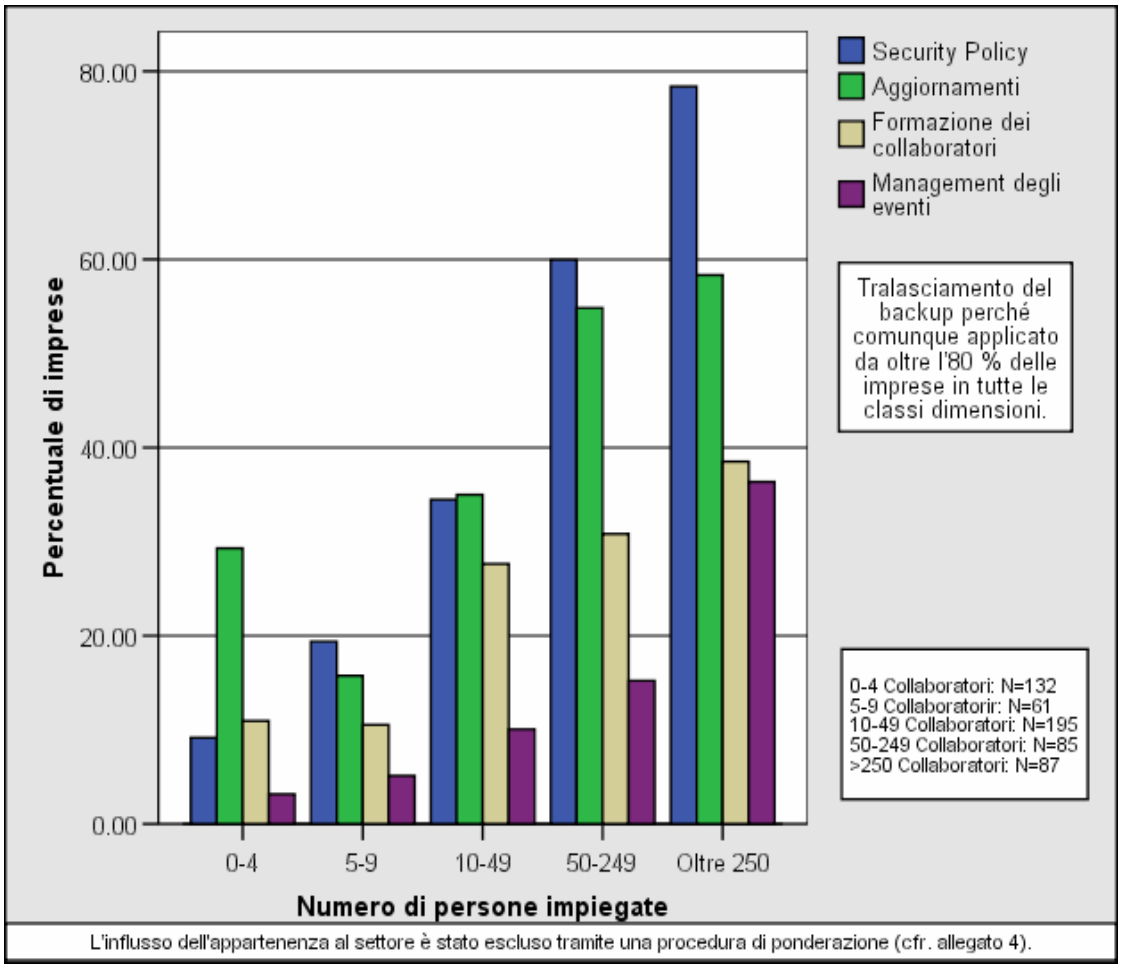
Formazione dei collaboratori
Un perfezionamento professionale regolare dei collaboratori nel settore della sicurezza dell'informazione può minimizzare il rischio di eventi correggendo i comportamenti errati. La formazione può essere impartita da specialisti interni o esterni, ma può anche limitarsi a campagne regolari di informazione.

3.1.4 L'applicazione di misure organizzative

L'inchiesta sulla diffusione delle diverse misure organizzative presso le imprese svizzere rivela che la salvaguardia dei dati è la principale preoccupazione delle imprese. Quasi tutte, ossia il 91 per cento, applicano un concetto di backup. Gli altri concetti sono applicati con minore frequenza. Il 39 per cento delle imprese ha definito una Security Policy e un Update Management, il 26 per cento provvede alla formazione dei collaboratori e il 13 per cento dispone di un management degli eventi.

Ancora una volta si tratta di esaminare con quale frequenza le diverse misure organizzative sono applicate dalle diverse imprese. Nella figura 5 l'influsso dovuto alle dimensioni dell'impresa è chiaramente visibile.

Figura 5 Applicazione di misure organizzative di protezione per categorie di dimensioni



È chiaramente visibile che, rispetto a quelle di piccole e medie dimensioni, le imprese più grandi applicano le misure organizzative con maggiore frequenza. Inoltre, nelle imprese di maggiori dimensioni è ancora più importante disciplinare in modo chiaro le responsabilità e elaborare direttive puntuali per tutti i collaboratori. Il management degli eventi cresce fortemente in funzione delle dimensioni dell'impresa. Il 36 per cento delle grandi imprese dispone di un management degli eventi. Ciò indica che rispetto alle imprese di dimensioni minori, per le grandi imprese è più importante ripristinare il più rapidamente possibile la prontezza di impiego dell'informatica dopo un evento. Nondimeno un numero relativamente elevato di grandi imprese, ossia il 64 per cento delle imprese che hanno risposto, rinuncia al management degli eventi.

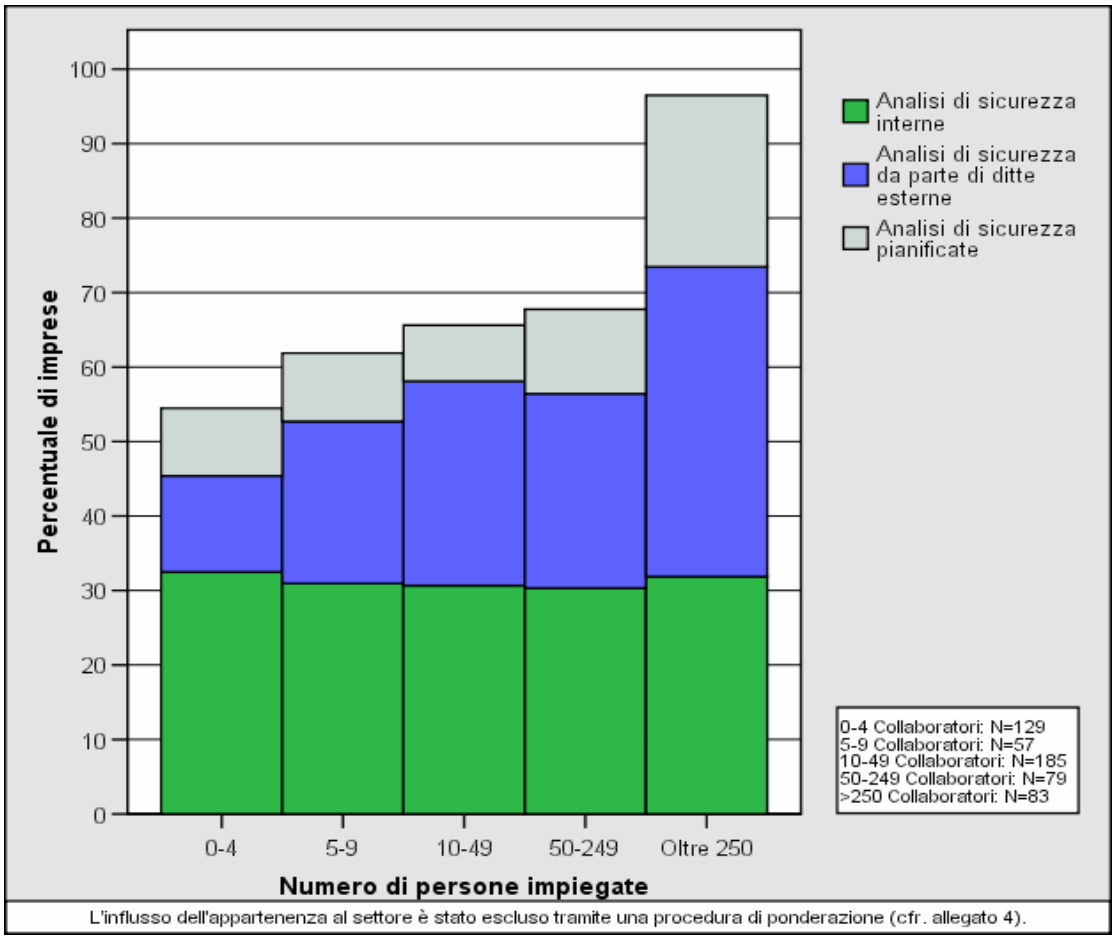
3.1.5 La verifica delle misure adottate

Un importante concetto di sicurezza – esaminato in modo separato in questa sede – è la verifica costante delle misure adottate. Soltanto chi analizza regolarmente tutte le misure per tutelare la sicurezza dell'informazione constata abbastanza precocemente le lacune e può reagire prima che queste siano all'origine di problemi. Il 56 per cento delle imprese interrogate effettua regolarmente simili analisi (il 32% a livello interno e il 24% ricorrendo a ditte esterne). L'11 per

cento delle imprese interrogate prevede di effettuare, in futuro, simili analisi di sicurezza[29]. Un terzo delle imprese non effettua né prevede di effettuare una verifica regolare.

Da un esame dettagliato risulta ancora una volta che soprattutto le grandi imprese verificano in modo conseguente la loro sicurezza. Come illustrato nella figura 6, il 72 per cento delle grandi imprese compie già analisi di sicurezza, mentre il 13 per cento indica di averne in programma.

Figura 6 Diffusione delle analisi di sicurezza per dimensioni delle imprese



La percentuale elevata di grandi imprese che effettuano analisi della sicurezza spicca sulla percentuale piuttosto modesta di imprese di medie dimensioni. È evidente che le grandi imprese hanno riconosciuto per prime l'importanza della verifica costante delle misure di sicurezza o che dispongono delle risorse necessarie a tale scopo.

Per un confronto con questi valori rinviamo allo studio «Hi-Tech Crime». Da questa inchiesta sulle imprese britanniche con oltre 100 collaboratori risulta che il 33 per cento di esse non effettua nessuna analisi della sicurezza[30]. Le grandi imprese hanno quindi un comportamento analogo a quello delle ditte svizzere in ambito di analisi della sicurezza (il 28% delle grandi imprese svizzere non analizza ancora la propria sicurezza).

29 Dalla ponderazione di questi risultati in funzione delle dimensioni e del settore (cfr. allegato 3) risulta che la percentuale di tutte le imprese svizzere che effettuano un'analisi della sicurezza può essere stimata al 47%. Un ulteriore 8% prevede di effettuare, in futuro, un'analisi della sicurezza.

30 National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005), pag. 29.

3.2 Le spese dell'impresa per la sicurezza dell'informazione

Le misure descritte qui sopra determinano in parte costi importanti. Poiché la minaccia è in continua mutazione, le imprese devono adeguare costantemente le loro misure tecniche e organizzative. Occorre inoltre mettere a disposizione e formare il personale. È ovvio che le imprese tentino di ridurre nella misura del possibile i costi della sicurezza dell'informazione. Perciò il dispendio finanziario che le imprese vi consacrano è un buon indicatore per verificare l'importanza che esse attribuiscono alla sicurezza dell'informazione. La stessa considerazione vale anche per le spese per il personale; in questo caso però non va considerato unicamente il numero di collaboratori, ma anche lo stato di formazione dei responsabili della sicurezza dell'informazione.

3.2.1 Il costo finanziario della sicurezza dell'informazione

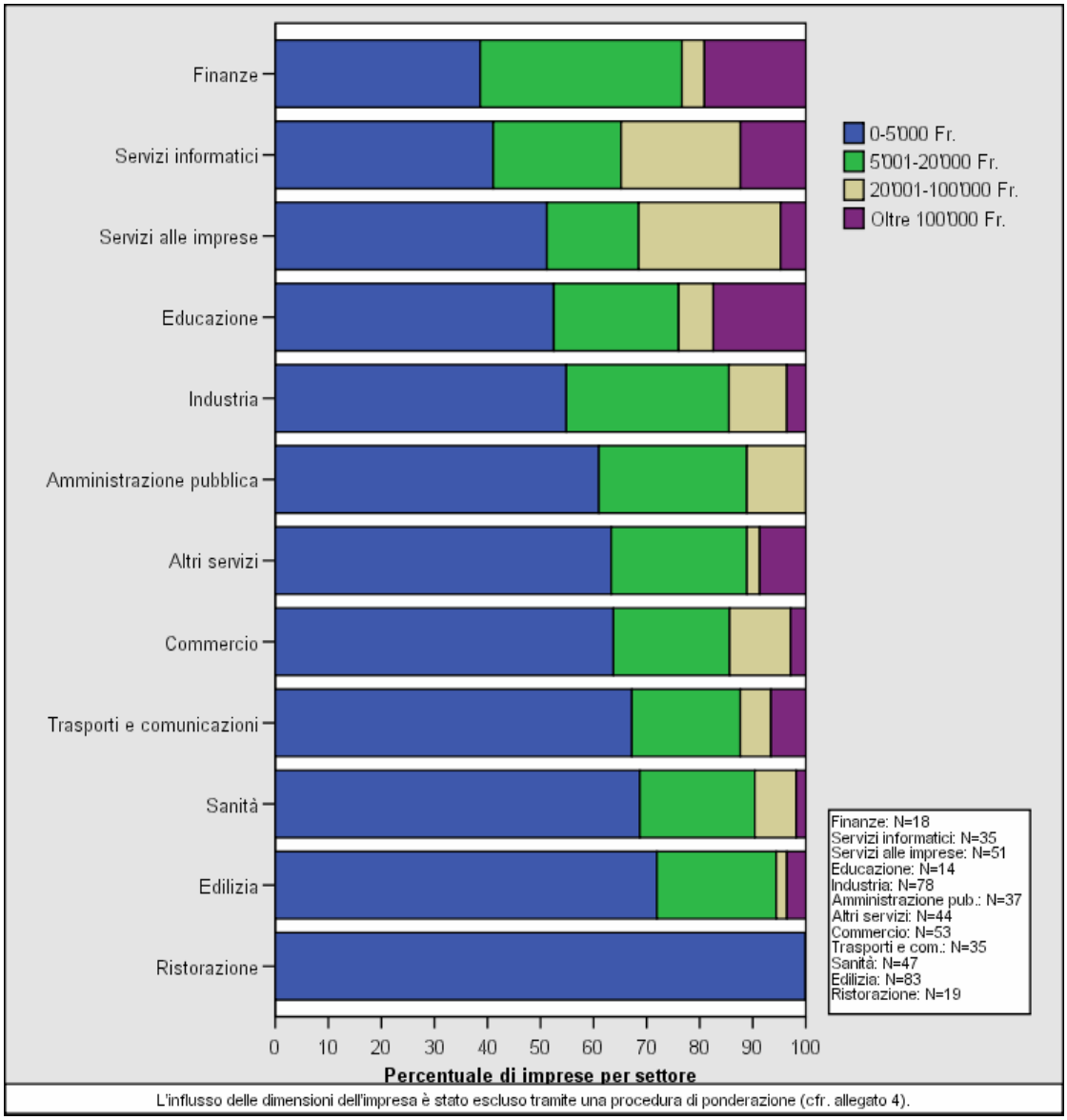
Nel quadro dell'inchiesta i dati relativi ai costi della sicurezza dell'informazione sono stati rilevati con l'ausilio di quattro categorie (0–5 000 fr.; 5 001–20 000 fr.; 20 001–100 000 fr.; oltre 100 000 fr.), poiché solo poche imprese sono in grado di fornire cifre precise. Dall'analisi di questi dati risulta che numerose imprese dispongono unicamente di risorse finanziare limitate per garantire la sicurezza dell'informazione. Il 62 per cento delle imprese che hanno fornito indicazioni sulle loro spese per la sicurezza dell'informazione indicano di non consacrare più di 5 000 franchi a questo scopo. Solo il 5 per cento di esse indica una spesa superiore a 100 000 franchi. Un'analisi dettagliata illustrerà ora quali imprese investono quante risorse finanziarie nel management dei rischi.

Sorprende poco il forte nesso tra le dimensioni dell'impresa e il dispendio finanziario per la sicurezza dell'informazione. Quanto più è grande l'impresa, tanto più essa investe nel management dei rischi[31]. Sulla base della maggiore consistenza dei loro preventivi, le grandi imprese dispongono di risorse finanziarie maggiori in ambito di sicurezza dell'informazione. Il loro maggiore dispendio è però anche giustificato se, come rilevato nel capitolo precedente, le grandi imprese devono in definitiva affrontare un numero sensibilmente maggiore di eventi rispetto alle piccole e medie imprese.

Oltre alle dimensioni, anche l'attività dell'impresa può avere un influsso sull'impegno finanziario a favore della sicurezza dell'informazione. Nel quadro dell'esame sulla frequenza degli eventi in funzione del settore è già stata formulata l'ipotesi che le imprese del settore finanziario registrano un numero di eventi pari a quello delle imprese del settore della ristorazione unicamente perché si proteggono meglio contro le minacce alla sicurezza dell'informazione. Per le imprese del settore finanziario la sicurezza dei dati assume normalmente un ruolo di importanza maggiore che non per le imprese del settore della ristorazione. La figura 7 illustra il dispendio delle imprese dei diversi settori per la sicurezza dell'informazione.

31 L'intensità del grado di correlazione tra le dimensioni dell'impresa e il dispendio per la prevenzione può essere espresso con il coefficiente di correlazione gamma. In caso di correlazioni positive (quanto più intensa la correlazione, tanto maggiore il coefficiente) il coefficiente gamma può raggiungere valori compresi tra 0 e 1. Nel caso della fattispecie oggetto dell'inchiesta si raggiunge un valore elevato, ovvero lo 0,791.

Figura 7 Dispendio finanziario per la sicurezza dell'informazione per settori



Tra i diversi settori esistono effettivamente notevoli differenze. Le imprese dei rami menzionati qui sopra costituiscono gli estremi: nel settore della ristorazione nessuna impresa consacra oltre 5 000 franchi alla sicurezza dell'informazione, mentre il 19 per cento delle imprese del settore finanziario investe oltre 100 000 franchi. In genere si può affermare che le imprese dei settori che considerano meno importante l'informatica investono conseguentemente anche meno nella sicurezza dell'informazione.

3.2.2 Il costo del personale per la sicurezza dell'informazione

Nel quadro dell'inchiesta sono state poste alle imprese due domande sul loro personale per la sicurezza dell'informazione. Si trattava di indicare innanzitutto le spese per il personale in questo

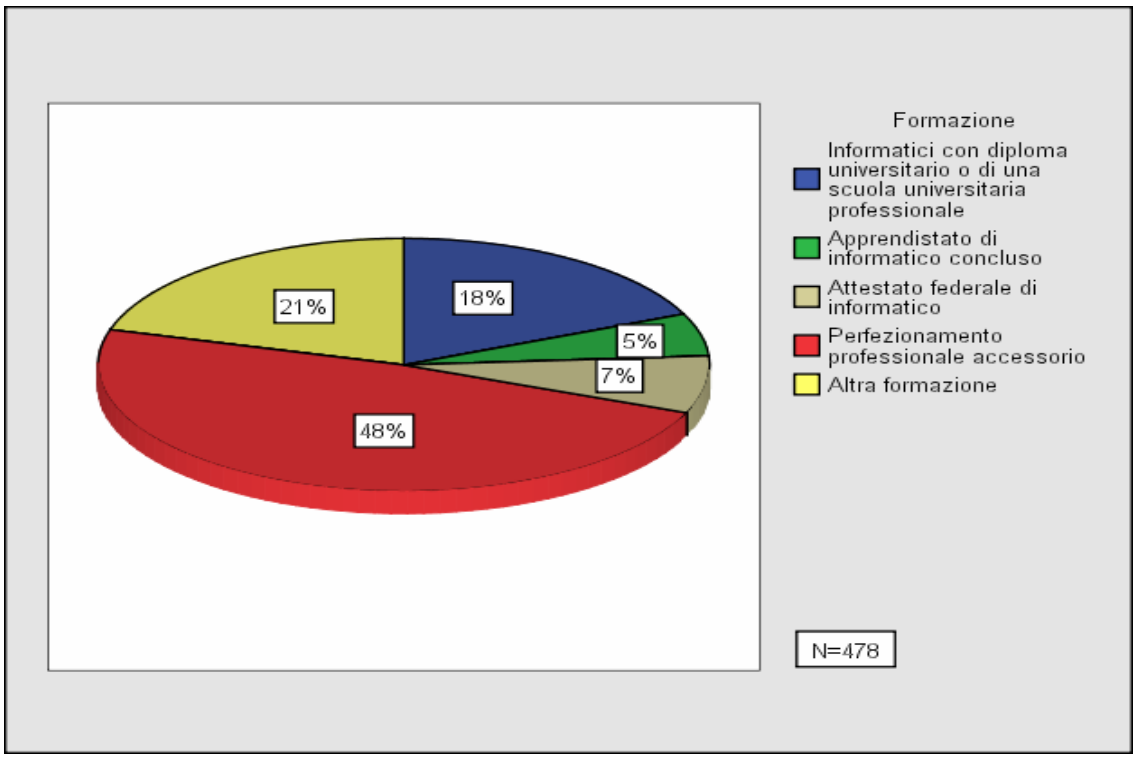
ambito in funzione del numero di posti a tempo pieno[32] e secondariamente lo stato di formazione del capo del team responsabile della sicurezza dell'informazione.

Le risposte relative alle dimensioni del team responsabile della sicurezza dell'informazione evidenziano che nella maggior parte delle imprese solo poco personale è assunto a tale scopo. In seno al 13 per cento delle imprese che hanno fornito indicazioni in merito, nessuno dei collaboratori si occupa direttamente della sicurezza dell'informazione. Il 60 per cento delle imprese indica di avere a disposizione al massimo 100 punti percentuali di posto. Un quarto appena delle imprese (24%) occupa piccoli team di 2–5 collaboratori e solo poche imprese (3%) occupano oltre cinque persone in questo ambito[33]. La sicurezza dell'informazione è quindi raramente definita come compito autonomo nella politica del personale delle imprese. Si ritiene che ne sia frequentemente responsabile la mancanza di risorse finanziarie; in parte però le imprese preferiscono soluzioni più flessibili (consulenza esterna, outsourcing) all'assunzione di un team.

Parallelamente alle risorse impiegate, anche le spese per il personale aumentano in funzione delle dimensioni dell'impresa[34]. Anche questa circostanza è riconducibile al fatto che le imprese di maggiori dimensioni dispongono di maggiori risorse finanziarie e di personale. Ciò non significa però che la maggiore disponibilità di risorse finanziarie comporti automaticamente maggiori spese per il personale. L'analisi delle spese per il personale in funzione del settore evidenzia infatti che le imprese del settore finanziario consacrano invero ingenti somme di denaro alla sicurezza dell'informazione, ma nel contempo impiegano per questo compito risorse piuttosto scarse in termini di personale[35]. È evidente che in alcuni settori sono preferite le soluzioni di outsourcing. Questa circostanza sarà esaminata più dettagliatamente in seguito.

Anzitutto si tratta di esaminare lo stato di formazione dei responsabili della sicurezza dell'informazione. Ai fini di una protezione efficace esso può essere altrettanto decisivo quanto le dimensioni del team. Gli specialisti costano però caro e possono essere impiegati in maniera meno flessibile. Per questo motivo non tutte le imprese possono permettersi specialisti.

Figura 8 Formazione dei responsabili della sicurezza dell'informazione



La figura 8 evidenzia che in meno di un terzo delle imprese un informatico diplomato è responsabile della sicurezza dell'informazione. Da un'osservazione più dettagliata risulta addirittura che questa percentuale potrebbe essere inferiore. Nel caso delle grandi imprese e delle imprese del settore informatico sono infatti impiegati più sovente informatici diplomati. Se si considera però il fatto che le grandi imprese sono rappresentate in proporzione eccessiva tra le imprese partecipanti all'inchiesta, la percentuale di informatici responsabili della sicurezza dell'informazione nelle imprese svizzere può essere stimata al 15 per cento soltanto [36].

L'esiguità della percentuale di specialisti formalmente qualificati può trasformarsi in un problema se le minacce divengono sempre più complesse. Da questo punto di vista la Svizzera non costituisce un caso isolato, poiché anche dallo studio britannico «Hi-Tech Crime» risulta che in ambito di sicurezza dell'informazione si avverte la mancanza di personale con qualifiche formali[37].

In merito alle spese per il personale in ambito di sicurezza dell'informazione si può affermare in sintesi che la maggior parte delle imprese occupa pochi collaboratori per questo compito e che solo presso una minoranza di esse la responsabilità principale incombe a un informatico diplomato.

3.3 Scorporamento del rischio

Come illustrato in precedenza, esistono imprese che investono invero ingenti risorse finanziarie nella sicurezza dell'informazione ma nel contempo assumono poco personale a tale scopo. È evidente che queste imprese fanno maggiormente capo a specialisti esterni, coprendo così in maniera più flessibile i bisogni in ambito di sicurezza dell'informazione. L'outsourcing non presenta però unicamente vantaggi. Poiché la protezione dell'informatica è prevalentemente un problema di management piuttosto che una questione di misure tecniche, una parte cospicua dei compiti in ambito di sicurezza dell'informazione permane presso l'impresa stessa. Inoltre la maggior parte degli specialisti dei partner di outsourcing è relativamente costosa.

Ogni impresa deve quindi valutare se la collaborazione con partner di outsourcing o l'impiego di un proprio team di sicurezza costituisce la soluzione migliore per garantire la sicurezza dell'informazione. Poiché per numerose imprese l'outsourcing rappresenta un importante complemento alle proprie misure, ne viene analizzata qui di seguito la diffusione. Una seconda sezione esaminerà invece se le imprese si assicurano contro i danni eventuali di un evento. Il rischio può infatti essere scorporato anche tramite un'assicurazione, perché in tale caso i possibili danni finanziari dovrebbero essere assunti dall'assicuratore.

3.3.1 La diffusione della cooperazione con partner di outsourcing

Per rilevare l'importanza dell'outsourcing in ambito di sicurezza dell'informazione, ai partecipanti all'inchiesta si è chiesto che percentuale delle risorse finanziarie consacrate alla sicurezza dell'informazione utilizzano per il pagamento di partner di outsourcing.

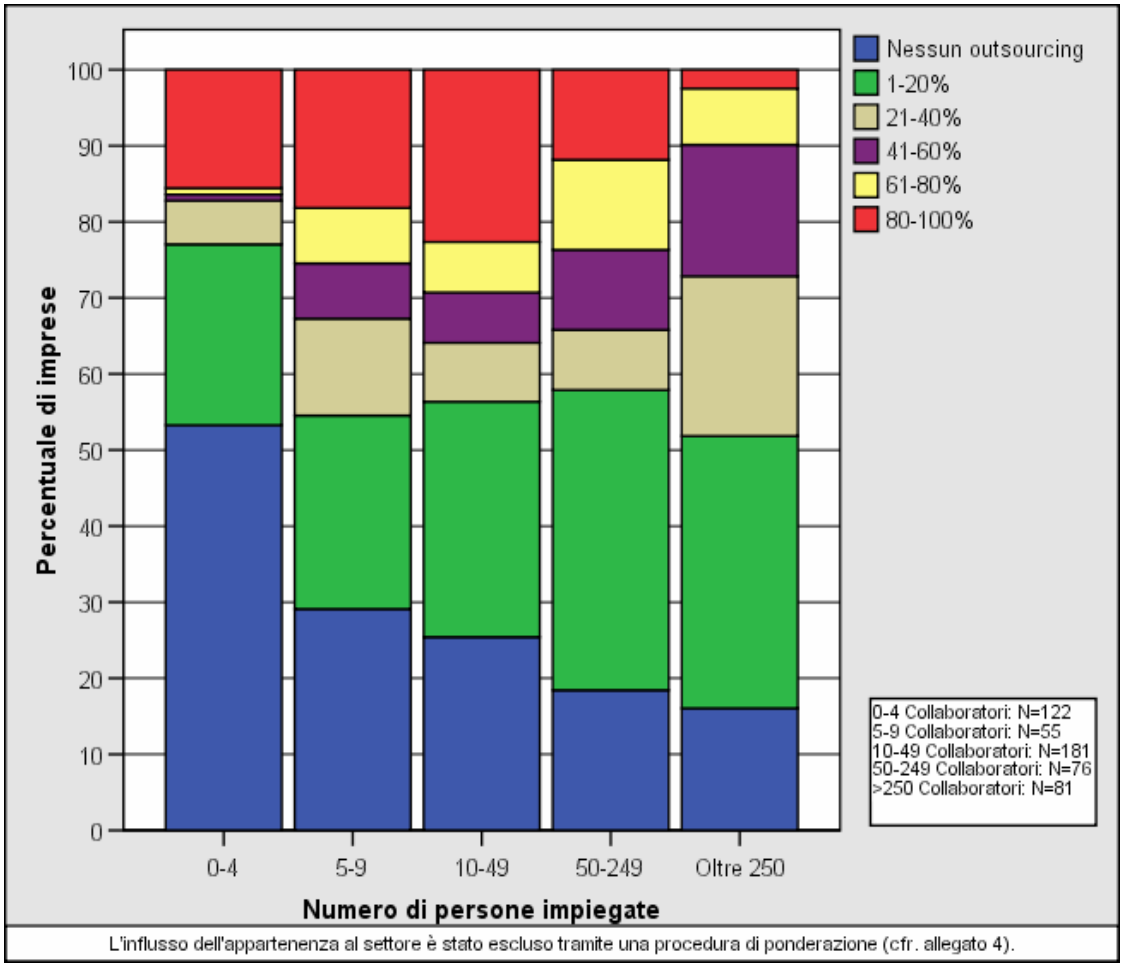
Il 30 per cento delle imprese interrogate indica che non pratica l'outsourcing. Un ulteriore 31 per cento vi consacra al massimo il 20 per cento del suo dispendio per la sicurezza dell'informazione. Oltre la metà delega pertanto soltanto una piccola parte della sua sicurezza

36 Questa stima risulta se si applica la procedura di ponderazione (cfr. allegato 3).

37 National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005), pag. 30.

informatica a specialisti, mentre il 15 per cento delle imprese consacra oltre l'80 per cento delle risorse finanziarie per la sicurezza informatica al pagamento di partner di outsourcing. La differenze tra le imprese sono molto marcate. È ancora più interessante analizzare quali imprese prediligono l'outsourcing. La figura 9 illustra la diffusione dell'outsourcing per categorie di dimensioni.

Figura 9 Outsourcing in funzione delle dimensioni delle imprese



Le microimprese con meno di cinque collaboratori praticano raramente l'outsourcing su vasta scala. Oltre la metà di queste imprese si occupa esclusivamente in modo autonomo della sicurezza dell'informazione. È probabile che l'outsourcing sia troppo caro per queste microimprese. È invece completamente diverso il comportamento delle piccole e medie imprese che scorporano una percentuale elevata della loro sicurezza dell'informazione. Più di un'impresa su cinque con 10–49 collaboratori scorpora almeno l'80 per cento del suo dispendio per la sicurezza dell'informatica. Parte di queste imprese di medie dimensioni dipende fortemente dall'informatica e ha inoltre poche possibilità di garantirne la sicurezza. Le grandi imprese invece collaborano sovente con partner di outsourcing, ma delegano raramente oltre il 60 per cento della loro sicurezza informatica (solo il 10% delle grandi imprese delega una simile percentuale).

L'osservazione della diffusione dell'outsourcing in funzione del settore conferma che le imprese del settore finanziario che consacrano ingenti somme di denaro alla sicurezza dell'informazione – ma assegnano poco personale a questo compito – praticano l'outsourcing in misura superiore alla media. È comprensibile che le imprese del settore informatico praticano solo

raramente l'outsourcing in ambito di sicurezza dell'informazione perché dispongono esse stesse di sufficiente know-how[38].

Non esistono studi internazionali paragonabili, che consentirebbero di desumere se le imprese svizzere praticano l'outsourcing in larga o scarsa misura. Da un confronto con gli «Computer Crime and Security Survey 2005» annuali dell'FBI e del CSI risulta una percentuale chiaramente più elevata di outsourcing per la Svizzera. I risultati non possono tuttavia essere direttamente confrontati a causa della speciale composizione dei partecipanti all'inchiesta dell'FBI[39].

3.3.2 La copertura tramite assicurazioni

Uno speciale caso di outsourcing è costituito dalle assicurazioni. In questo contesto i costi eventuali dei danni dovuti ad attacchi contro la sicurezza dell'informazione sono scorporati. In Svizzera sono offerte fin dal 2000[40] assicurazioni per coprire i rischi di Internet. I risultati dell'inchiesta evidenziano che questo tipo di assicurazione si è rapidamente affermato: il 45 per cento delle imprese che hanno risposto a questa domanda indica di avere sottoscritto un'assicurazione per i danni eventuali alla struttura informatica. Sulla scorta di queste indicazioni è possibile stimare che circa un terzo di tutte le imprese ha concluso una simile assicurazione[41].

Le assicurazioni sono soprattutto diffuse presso le medie imprese con 50–249 collaboratori; il 69 per cento di queste imprese ha concluso un'assicurazione per coprire questi rischi. Nel caso delle microimprese la percentuale è inferiore (29%) e anche le grandi imprese sono assicurate con una frequenza assai minore (54%). Le più frequentemente assicurate sono le amministrazioni pubbliche, seguite dalle imprese del settore finanziario e dalle aziende che forniscono servizi alle imprese.

Le imprese che non si assicurano adducono soprattutto motivazioni di carattere economico. Oltre la metà di esse (55%) ha indicato che un'assicurazione non sarebbe proficua nel loro caso. Il 29 per cento di queste imprese non era semplicemente a conoscenza dell'offerta di simili assicurazioni. Il 15 per cento ha indicato di non disporre delle risorse finanziarie per un'assicurazione, mentre un ulteriore 8 per cento (soprattutto grandi imprese) considera insufficienti le offerte delle compagnie di assicurazione[42].

Anche per quanto concerne la copertura dei rischi tramite assicurazione mancano dati internazionali di confronto. Nondimeno, pur senza possibilità di confronto si può constatare che la copertura è sorprendentemente elevata. Numerose imprese hanno concluso un'assicurazione sebbene le offerte in questo campo esistano soltanto da pochi anni.

38 Soltanto il 9% delle imprese del settore informatico consacra all'outsourcing oltre il 40% dei suoi costi in ambito di sicurezza dell'informazione.

39 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005), pag. 9. I partecipanti a questo studio dell'FBI/CSI sono membri del Computer Security Institute (CSI). Si può pertanto desumere che in ambito di sicurezza dell'informazione essi profondono sforzi autonomi superiori alla media. Nel quadro di questo studio sono peraltro state prevalentemente interrogate grandi imprese.

40 Haldemann, Lukas, V*ersicherung von Internet-Risiken* (lavoro di seminario al Dipartimento di informatica del PF di Zurigo, 2001), pag. 5.

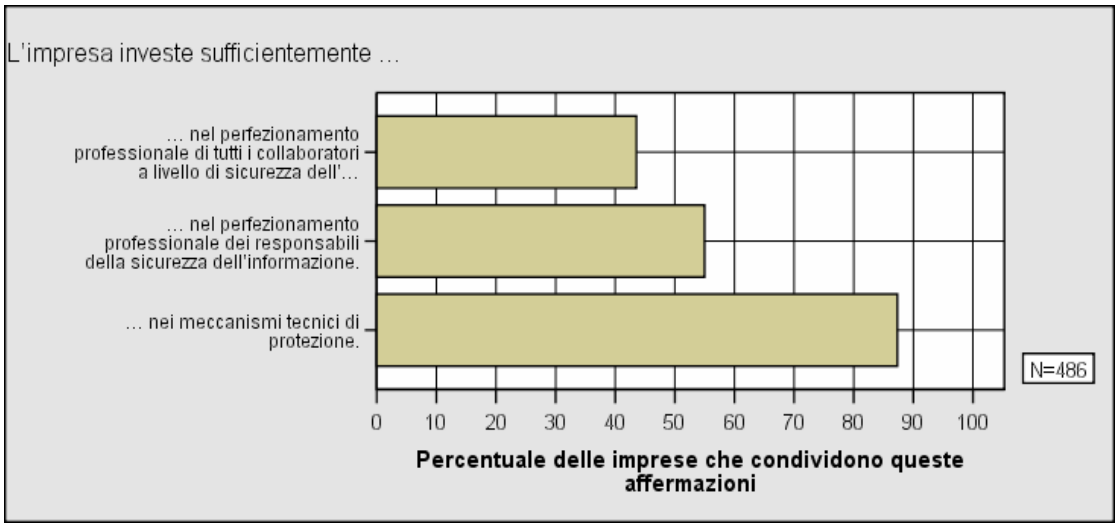
41 Questa stima risulta ancora una volta dalla ponderazione dei dati dell'inchiesta in funzione delle dimensioni delle imprese e del settore (cfr. allegato 3).

42 Si potevano selezionare diverse risposte.

3.4 Conclusioni relative al management dei rischi da parte delle imprese

Il management dei rischi può essere strutturato in maniera molto diversificata. Quasi tutte le imprese applicano le misure di sicurezza più elementari (programmi antivirus, firewall, backup). Alcune imprese, soprattutto quelle di minori dimensioni, si accontentano di questi provvedimenti, mentre altre imprese hanno un maggiore bisogno di protezione e lo coprono sia esse stesse con misure tecniche e organizzative supplementari, sia facendo capo a partner di outsourcing. Poiché esistono numerose modalità di implementazione del management dei rischi, non è possibile valutarne la qualità per l'insieme delle imprese. È altresì impossibile constatare un effetto diretto delle misure adottate sulle probabilità di un evento. Questa circostanza è dovuta al fatto che le imprese che hanno adottato il maggior numero di misure sono anche quelle maggiormente esposte al rischio di un evento. Inoltre gli eventi possono in parte essere effettivamente scoperti soltanto grazie all'ausilio delle misure di protezione. L'87 per cento delle imprese condivide l'affermazione secondo la quale la propria azienda investe sufficientemente nelle misure tecniche di protezione. Come risulta dalla figura 10, la soddisfazione in ambito di formazione non è affatto identica: sola un'esigua maggioranza di imprese è soddisfatta dell'impegno profuso nella formazione dei responsabili della sicurezza dell'informazione e una minoranza ritiene addirittura che non si investe sufficientemente nel perfezionamento professionale dei collaboratori generici.

Figura 10 Valutazione dei propri investimenti nella sicurezza dell'informazione



Ovviamente anche la soddisfazione delle imprese per i loro propri investimenti dice ben poco sulla qualità effettiva del management dei rischi. È però evidente che un grande numero di imprese ha riconosciuto che la sicurezza dell'informazione non è unicamente un problema tecnico, ma che occorre anche investire nella formazione[43].

Alla fine di questo capitolo – anche se non è possibile valutare in modo esauriente la qualità del management dei rischi – bisogna ricordare ancora una volta alcuni punti importanti:

43 I risultati corrispondono a un'inchiesta condotta dalla KPMG sulla soddisfazione di CIOs (Chief Information Officers) prescelti in merito alla sicurezza dell'informazione nelle loro imprese. Anche da questa inchiesta risulta una grande soddisfazione per le misure tecniche e una profonda soddisfazione per il sentimento di sicurezza degli utenti finali. KPMG, *IT-Management 2005* (Zurigo e Ginevra, 2005), pag. 26.

le imprese svizzere scorporano in misura relativamente frequente parti della loro sicurezza dell'informazione (soprattutto le medie imprese). Un motivo di scorporamento è il fatto che, di solito, per la sicurezza dell'informazione sono disponibili solo pochi punti percentuali di posto e che sovente i collaboratori non sono informatici diplomati. Soprattutto le medie imprese non possono affatto permettersi tutte le misure necessarie. A causa dell'esiguità delle risorse e nell'ipotesi che numerosi responsabili abbiano bisogno di perfezionamento professionale è importante sapere se le imprese sono interessate a cooperazioni in ambito di sicurezza dell'informazione.

4 Aiuto esterno e cooperazione

Nei capitoli precedenti è emerso chiaramente che per numerose imprese la sicurezza dell'informazione è un tema importante. La maggior parte delle imprese constata sempre nuovi eventi che pregiudicano la sicurezza della loro informatica. Per fare fronte a questi eventi le imprese dipendono sovente dal ricorso ad aiuti esterni. Occorre pertanto dapprima esaminare la frequenza con la quale le imprese ricorrono ad aiuti esterni e dove li trovano.

Non soltanto nel caso degli eventi, ma anche in quello del management dei rischi le imprese pervengono ai limiti delle loro capacità. Una protezione effettiva ed efficiente dell'informatica è cara e deve essere costantemente adeguata. Poiché numerose imprese devono affrontare problemi analoghi, ci si chiede se non sarebbe sensato uno scambio reciproco. Pertanto viene pure esaminato quali imprese sarebbero disposte a una collaborazione, chi la dovrebbe coordinare e come dovrebbe essere finanziata. In questo contesto sarà esaminato dettagliatamente anche il ruolo dello Stato. In merito ci si chiede anzitutto quali contributi potrebbe fornire lo Stato per sostenere le imprese in questo ambito.

4.1 Aiuto esterno in caso di eventi

Già nel quadro dell'esame della percentuale di imprese con partner di outsourcing si è potuto constatare che in ambito di management dei rischi le imprese svizzere dipendono sovente dalle competenze di altre imprese. Tale frequenza si accentua se si verifica un evento che minaccia la sicurezza dell'informazione. Per le imprese può però anche risultare problematico sollecitare un simile aiuto perché i segreti aziendali potrebbero pervenire al pubblico o perché l'immagine dell'impresa potrebbe subirne un danno. Ci si chiede pertanto se le imprese con problemi di sicurezza dell'informazione debbano effettivamente sollecitare aiuti esterni e, nell'affermativa, presso chi.

I risultati dell'inchiesta evidenziano che il 63 per cento delle imprese che hanno constatato un evento rilevante ai fini della loro sicurezza dell'informazione hanno fatto capo a un aiuto esterno[44]. Le imprese medie con 10–49 collaboratori sono quelle che sollecitano più sovente aiuti esterni. Trova pertanto conferma la diagnosi tratta dall'esame della diffusione dell'outsourcing, secondo la quale le imprese di questa categoria di dimensioni dipendono con maggiore frequenza da sostegni di terzi. Da uno sguardo alla ripartizione per settori risulta che i partecipanti del settore delle amministrazioni pubbliche fanno capo molto sovente ad aiuti esterni (75%), mentre le imprese del settore informatico necessitano raramente di ulteriori sostegni (36%).

È altresì interessante sapere dove le imprese trovano l'aiuto necessario. La maggior parte delle imprese si rivolgono ai partner di outsourcing, ai produttori del loro software o al provider di Internet. Il 40 per cento delle imprese indica anche che effettua scambi con colleghi di altre imprese, mentre il 25 per cento cerca aiuto tramite Internet.

44 Ancora una volta questo risultato non può essere riportato direttamente sull'insieme delle imprese svizzere perché i partecipanti all'inchiesta non costituiscono una riproduzione proporzionale di tutte le imprese. Con l'ausilio della procedura di ponderazione (cfr. allegato 3) si può però stimare che circa la metà (47%) delle imprese svizzere colpite da un simile evento fanno capo ad aiuti esterni.

Risulta quindi che le imprese non ricercano sempre aiuti a pagamento presso esperti, ma sono pure interessate allo scambio reciproco. Occorre pertanto esaminare le modalità di strutturazione della cooperazione tra le imprese.

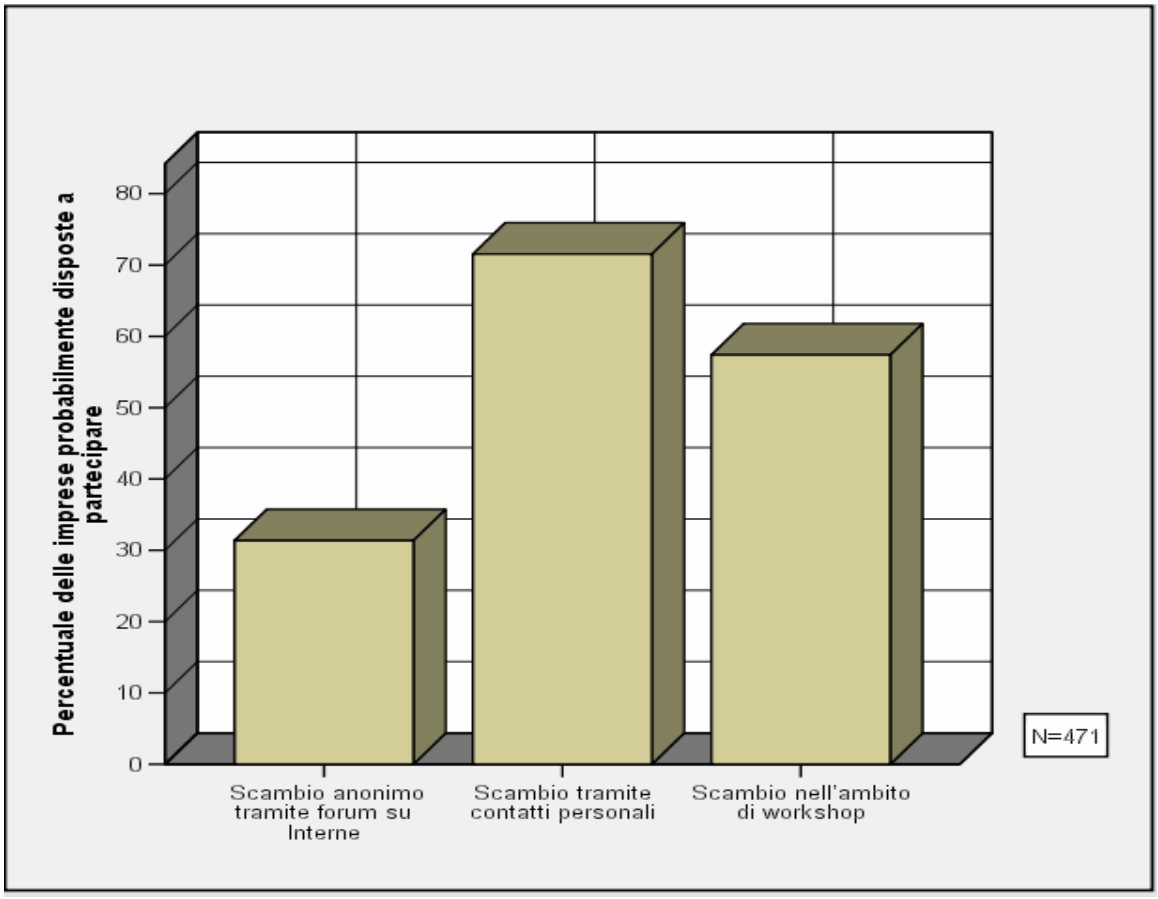
4.2 Cooperazione tra le imprese

Per capire quale collaborazione tra imprese sarebbe sensata bisogna delucidare diverse questioni. Si chiarisce innanzitutto a quali forme di cooperazione parteciperebbero le imprese e, secondariamente, chi dovrebbe coordinare la collaborazione. Infine, si esamina se vi è la disponibilità a fornire alla cooperazione anche risorse finanziarie.

4.2.1 Forme possibili di cooperazione

Affinché sia chiaro a quale forma di collaborazione sono disposte le imprese, i partecipanti all'inchiesta sono stati interrogati in merito. La scelta verteva sullo scambio anonimo tramite forum su Internet, sullo scambio tramite contatti personali e sullo scambio nel quadro di workshop. La figura 11 illustra i risultati di questa domanda.

Figura 11 Disponibilità di partecipazione in funzione delle forme di cooperazione



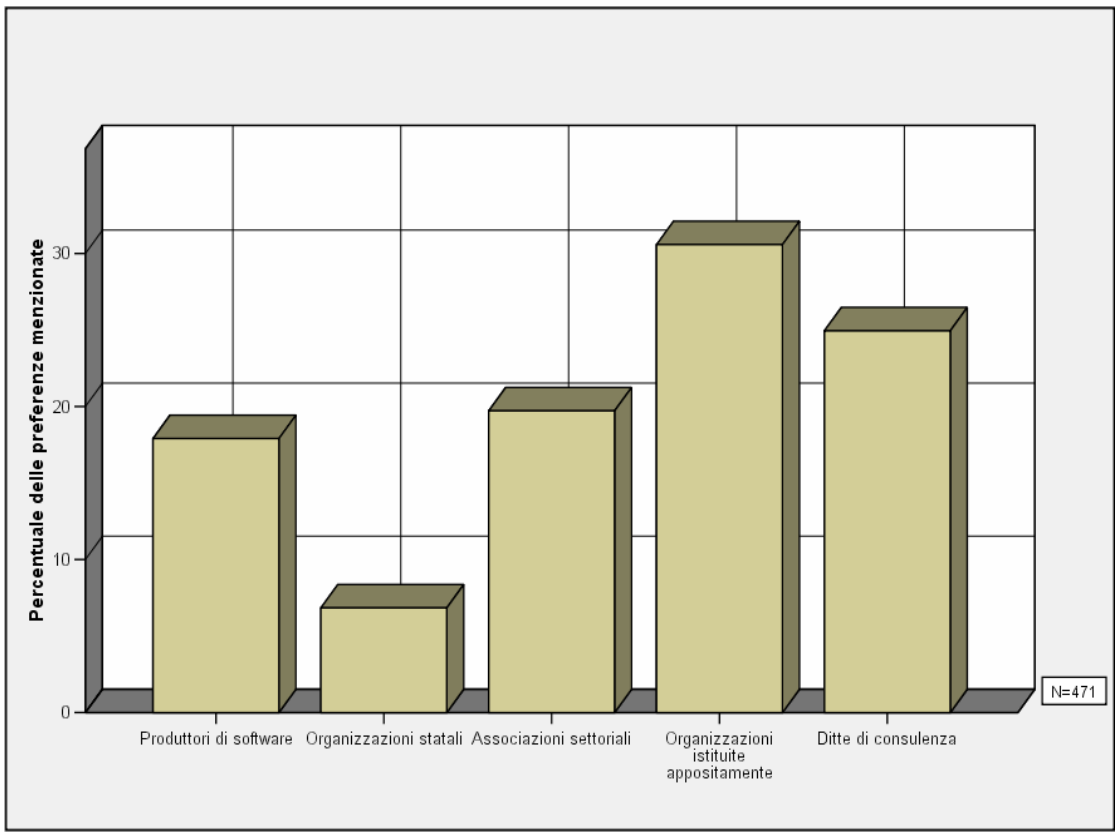
La maggiore disponibilità si constata a livello di cooperazione tramite contatti personali. Una maggioranza evidente parteciperebbe a uno scambio di questo genere. Anche l'idea di prendere parte a workshop suscita consensi[45]. Il forte interesse per uno scambio tra colleghi è degno di nota. È ovvio che i responsabili della sicurezza dell'informazione sono consapevoli dell'analogia dei problemi presso numerose imprese e del fatto che se ne potrebbe trarre reciprocamente profitto. Un terzo circa delle imprese interrogate (31%) può immaginarsi di discutere in Internet di questioni di sicurezza dell'informazione.

La necessità di una cooperazione risulta manifesta. È pertanto importante sapere chi dovrebbe assumere l'eventuale coordinamento della collaborazione e se le imprese sarebbero eventualmente disposte a fornire un contributo finanziario a una simile organizzazione.

4.2.2 L'organizzazione della cooperazione

Anche se numerose imprese auspicano una cooperazione, qualcuno deve essere disposto ad assumerne l'organizzazione. Alle imprese si è pertanto chiesto chi – a loro parere – sarebbe più idoneo a coordinare la collaborazione tra imprese sulla base di un centro di competenze. Quali possibili risposte sono stati proposti i produttori di software, le organizzazioni statali, le associazioni settoriali, le imprese di consulenza e le organizzazioni appositamente istituite. La figura 12 illustra quali attori ottengono le preferenze delle imprese interrogate.

Figura 12 Possibili organizzatori della cooperazione



45 È stata operata una distinzione tra workshop organizzati dai produttori di software e workshop organizzati da terzi indipendenti. Ai workshop dei produttori di software parteciperebbe il 41% delle imprese e a quelli organizzati da terzi indipendenti il 50%. Il grafico considera tutte le imprese che parteciperebbero all'una o all'altra possibilità.

Dall'inchiesta risulta che oltre il 30 per cento delle imprese ritiene che il coordinamento della collaborazione può essere garantito al meglio da organizzazioni istituite appositamente per questo scopo. Rimane per il momento aperta la questione della struttura di queste organizzazioni.

Il 25 per cento di tutte le imprese interrogate dà la preferenza a imprese di consulenza. Ma anche i produttori di software (18%) vanno menzionati, soprattutto perché collaborano con numerose imprese. Anche le associazioni settoriali sono citate con frequenza (20%). Esse hanno il vantaggio di avere già esperienza in ambito di coordinamento e di organizzazione.

Le microimprese danno la preferenza ai produttori di software e alle imprese di consulenza, mentre le piccole e medie imprese citano con maggiore frequenza le associazioni settoriali e soprattutto organizzazioni appositamente istituite per questi compiti[46]. È probabile che le imprese di dimensioni minori siano maggiormente interessate a una consulenza nel senso di una mediazione di conoscenze. Invece le medie e grandi imprese ricercano piuttosto una collaborazione con scambio reciproco.

Dalla valutazione dei risultati emerge chiaramente che la consulenza e l'assistenza dirette alla cooperazione non sono percepite come compito dello Stato. Il prossimo capitolo tratterà in modo più dettagliato il ruolo svolto dallo Stato. Ma prima verrà discussa la questione della disponibilità delle imprese a fornire un contributo finanziario all'organizzazione della collaborazione.

4.2.3 Il finanziamento della cooperazione

La domanda relativa al finanziamento della cooperazione è stata formulata in termini molto generali. Si trattava di rilevare se le imprese possono immaginare di versare fino a 500 franchi o fino a 2 000 franchi all'anno a organizzazioni che offrono informazioni sulla sicurezza dell'informazione e coordinano la collaborazione. Le indicazioni dovevano costituire l'espressione della disponibilità a compartecipare ai costi della cooperazione.

Poiché la domanda è stata formulata in maniera poco concreta e poiché alcune delle persone che hanno compilato le risposte non disponevano delle competenze sufficienti per decidere in merito agli impegni finanziari della loro impresa, la percentuale di imprese che non hanno potuto rispondere alla domanda è molto elevata (36%). Il 71 per cento delle imprese che hanno risposto ha dichiarato in definitiva che non era disposto a versare un contributo, mentre il 22 per cento è disposto a versare un contributo fino a 500 franchi e l'8 per cento un contributo fino a 2 000 franchi. Sono disposte a versare un contributo soprattutto le grandi imprese, perché un contributo modesto al finanziamento della cooperazione in ambito di sicurezza dell'informazione non è di grande rilievo nel caso di ingenti preventivi . Il 55 per cento delle grandi imprese sarebbe disposto a versare un contributo. Nel caso invece delle microimprese solo il 15 per cento sarebbe disposto a versare un contributo fino a 500 franchi.

Non sorprende affatto che la stragrande maggioranza respinga una partecipazione finanziaria, in particolare se si ricorda che i budget per la sicurezza dell'informazione della maggior parte delle imprese sono esigui. Nondimeno oltre la metà delle grandi imprese e un terzo delle medie imprese con 50–249 collaboratori si dichiarano disposte a partecipare ai costi della collaborazione in ambito di sicurezza dell'informazione. Ciò evidenzia ancora una volta la necessità – perlomeno

46 Il 29% delle piccole imprese e delle microimprese con meno di 10 collaboratori auspica offerenti di software come organizzatori della cooperazione, mentre un ulteriore 28% ritiene più idonee le imprese di consulenza. Il 43% delle grandi imprese considera necessaria un'apposita organizzazione.

per le grandi e medie imprese – di una più intensa cooperazione a livello di sicurezza dell'informazione.

4.3 Cooperazione con lo Stato

Il fatto di riconoscere che la sicurezza dell'informazione è un problema che concerne l'intera economia solleva altresì gli interrogativi seguenti: lo Stato può sostenere i provvedimenti di protezione delle imprese? In caso affermativo, in che modo dovrebbe sostenerli?

La protezione di infrastrutture di importanza centrale per il benessere della popolazione rientra nei compiti tradizionali dello Stato. La protezione delle infrastrutture di informazione è diventata un importante compito dello Stato perché nelle società moderne tale benessere dipende in misura preponderante dal funzionamento delle tecnologie dell'informazione e della comunicazione. Lo Stato può assolvere questo compito, noto a livello internazionale con il termine *Critical Information Infrastructure Protection* (CIIP), unicamente in collaborazione con le imprese dell'economia privata[47]. Esso è quindi interessato a collaborare con le imprese e a sostenerle nella protezione della loro informatica. Diversamente dalle imprese, lo Stato persegue tuttavia una strategia a lungo termine che va oltre la mera garanzia dell'attività commerciale.

Anche a motivo di questa diversità di prospettive in ambito di sicurezza dell'informazione ci si chiede se le imprese auspichino una collaborazione con lo Stato. Come già menzionato, solo poche imprese considerano lo Stato un attore idoneo al coordinamento della cooperazione tra imprese. Il ruolo dello Stato viene quindi giudicato in modo piuttosto critico dalle imprese. Per questi motivi è importante verificare l'intensità dell'attuale collaborazione tra Stato e imprese.

4.3.1 Il ruolo della polizia

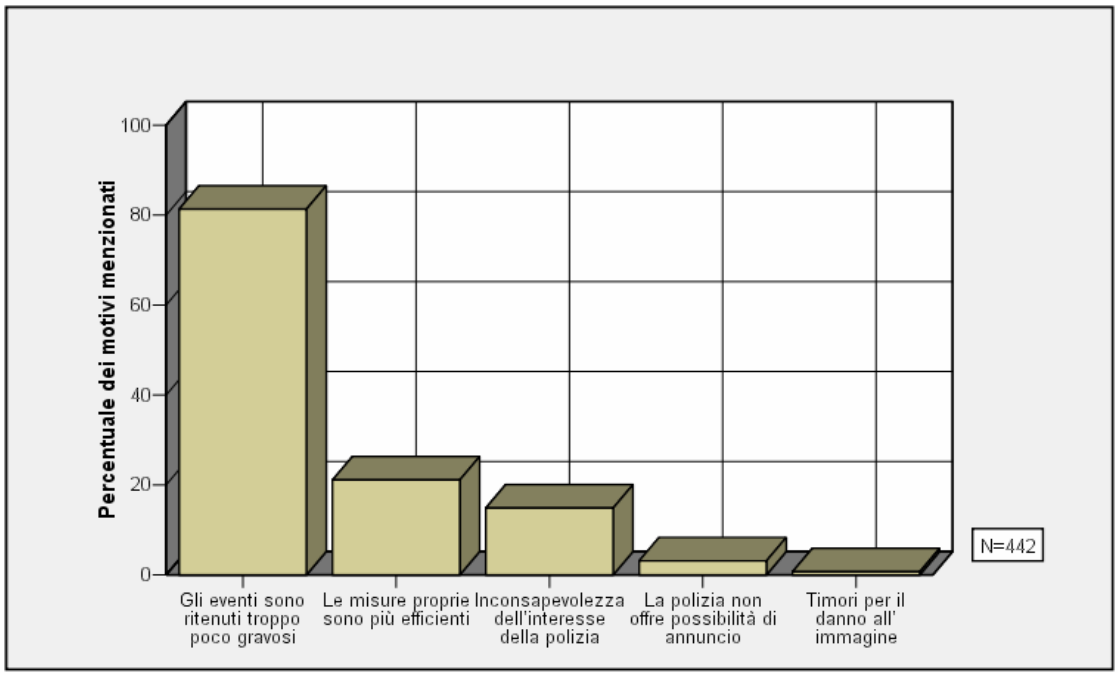
I privati o le imprese si rivolgono solitamente alla polizia se sono vittima di truffe o di furti, giacché essa è responsabile della garanzia della sicurezza nei confronti di reati contro il patrimonio. Ma le imprese si rivolgono alla polizia anche quando le loro strutture informatiche sono oggetto di un'aggressione o quando sono derubate dei loro dati?

Nel quadro dell'inchiesta si è analizzato se le imprese si sono già rivolte alla polizia a causa di un evento. Il risultato è chiaro: solo 34 delle 562 imprese interrogate (6%) hanno risposto affermativamente. Di queste 34 imprese 15 sono di grandi dimensioni. Nel raffronto internazionale si conferma il fatto che, in caso di evento concernente la sicurezza dell'informazione, le imprese informano solo molto raramente la polizia. Dal «Computer Crime Survey» dell'FBI risulta che in un simile caso il 9,1 per cento delle imprese statunitensi si rivolge alla polizia.

È ora interessante sapere per quale motivo questa percentuale è così bassa. A tale scopo le imprese sono state interrogate sulle ragioni per la quali non hanno fatto intervenire la polizia. La figura 13 illustra la frequenza con cui sono stati menzionati i motivi (si potevano indicare più motivi).

47 Maggiori informazioni sul tema della *Critical Information Infrastructure Protection* in: Abele-Wigert, Isabelle e Myriam Dunn, *The International Critical Information Infrastructure Handbook 2006* (Zurigo, 2006).

Figura 13 Motivi per i quali non è stata fatta intervenire la polizia



È probabile che molte imprese considerino troppo poco gravosi gli eventi dai quali sono state toccate per informarne la polizia. Per numerose imprese gli eventi che implicano malware fanno parte della quotidianità e non vengono pertanto annunciati. Sorprende parimenti poco che un'impresa su cinque ritenga più efficienti le proprie misure. È invece meno decisivo il comportamento della polizia. Solo poche imprese indicano di non avere fatto intervenire la polizia perché ritenevano che essa non si interessasse a questi casi o che non offrisse la possibilità di segnalarli. Degno di nota è pure il fatto che – contrariamente a un'opinione diffusa – il timore del danno all'immagine dell'impresa non distoglie affatto le imprese dall'annunciare l'evento.

Ancora una volta questi risultati sono confermati dal confronto con il «Computer Crime Survey» dell'FBI. Anche in tale contesto il motivo principale che induce le imprese a non fare intervenire la polizia è il fatto che gli eventi sono considerati troppo poco gravosi[48].

4.3.2 La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI)

Solo in pochissimi casi le imprese considerano pertanto sensato l'intervento della polizia. Numerosi problemi di sicurezza non possono però affatto essere risolti dalle autorità convenzionali di perseguimento penale. Per questo motivo lo Stato ricerca altre forme di sostegno all'economia in ambito di sicurezza dell'informazione. A questo scopo è stata istituita la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI). Operando in collaborazione con le organizzazioni dell'economia e delle autorità, MELANI ha il compito di individuare il più presto possibile i pericoli e le minacce e di offrire alle imprese la possibilità di annunciare gli eventi[49]. MELANI ha iniziato la sua attività il 1° ottobre 2004. Essa pubblica regolarmente sulla

48 Federal Bureau of Investigation (FBI), *2005 FBI Computer Crime Survey* (2005), pag. 12.

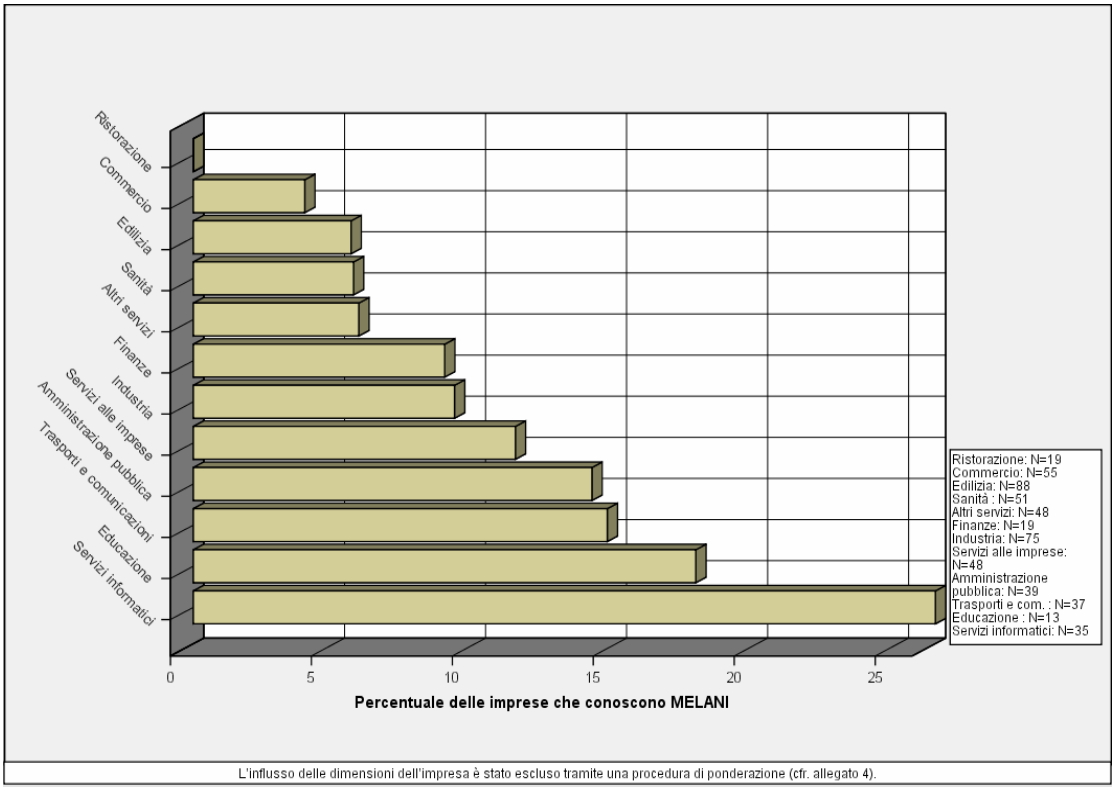
49 I principali partner in questo contesto sono l'Organo strategia informatica della Confederazione (OSIC) , il Servizio di analisi e di prevenzione (SAP) dell'Ufficio federale di polizia nonché il Computer Emergency Response Team della fondazione Switch (www.switch.ch).

sua homepage informazioni sulla situazione di minaccia del momento e avvertimenti in merito a nuovi pericoli[50]. È ovvio che queste indicazioni sono di ausilio soltanto se sono effettivamente osservate dalle imprese. Pertanto è di somma importanza conoscere il grado di notorietà di MELANI presso le imprese a poco più di un anno dalla sua istituzione.

Il 10 per cento delle imprese interrogate conosce MELANI. In merito va osservato che MELANI collabora strettamente con alcuni grandi esercenti di infrastrutture critiche. Essi non hanno partecipato all'inchiesta.

La percentuale delle imprese che conoscono MELANI aumenta considerevolmente in proporzione alle loro dimensioni. Se la percentuale di notorietà di MELANI è solo del 4 per cento nel caso delle microimprese con meno di cinque collaboratori, essa sale pur sempre al 28 per cento nel caso delle grandi imprese. Come illustrato dalla figura 14, sussistono notevoli differenze anche tra i diversi settori.

Figura 14 Notorietà di MELANI per settori



MELANI è conosciuta soprattutto dalle imprese del settore informatico. Nel corso del suo primo anno di esistenza MELANI ha raggiunto un grado di notorietà già relativamente elevato presso le imprese che si occupano intensamente del tema della sicurezza dell'informazione.

Per MELANI è difficile rispondere a tutti i bisogni perché il problema della sicurezza dell'informazione assume aspetti di qualità e di quantità diversi a seconda delle dimensioni e del settore delle imprese. Se le grandi imprese necessitano di una consulenza specifica tra specialisti, le medie imprese sono piuttosto interessate a consigli di portata generale. Nelle conclusioni di questo studio verranno illustrate in maniera più approfondita le possibili soluzioni di questo problema.

50 www.melani.admin.ch.

5 Conclusioni

L'obiettivo del presente studio era presentare una sintesi delle minacce che gravano sull'informatica delle imprese svizzere e delle modalità di protezione. Le analisi hanno mostrato che le minacce alla sicurezza dell'informazione sono molto diffuse e che il management dei rischi in questo ambito è un tema importante per tutte le imprese. È pure risultato evidente che sussistono differenze fondamentali tra le imprese. Questo ultimo capitolo discuterà le conclusioni che devono essere tratte da questi risultati.

5.1 Minacce diverse – management dei rischi diverso – esigenze diverse

La conclusione più importante a cui giunge il presente studio è che le minacce in ambito di sicurezza dell'informazione possono assumere un peso molto diverso per le varie imprese. L'appartenenza settoriale delle imprese è un fattore di una certa rilevanza, ma ben più importanti sembrano essere le dimensioni delle stesse. Mentre le piccole e medie imprese sono toccate soprattutto dal malware, nel 2005 una grande impresa su cinque aveva già constatato un attacco mirato alle sue strutture informatiche. Nella valutazione dei risultati si deve pertanto distinguere tra grandi imprese, aziende medie e microimprese.

5.1.1 Le microimprese

Le microimprese con meno di cinque collaboratori sono le meno toccate dalle minacce alla sicurezza dell'informazione. Il loro esercizio dipende sovente in maniera meno intensa dall'informatica rispetto alle grandi imprese e nella maggior parte dei casi sono di scarso interesse per gli hacker. Per esse la protezione elementare è dunque di grande importanza. Spesso misure tecniche dispendiose e piani di sicurezza complessi sono poco opportuni. Pertanto si può presupporre che le microimprese dispongano di un'autonomia relativamente elevata in ambito di sicurezza dell'informazione, ossia esse stesse possono attuare il necessario. Potrebbero invece essere di grande ausilio per le microimprese raccomandazioni impostate sulla prassi e, eventualmente, corsi di formazione, considerato che solo in pochi casi esse occupano informatici.

5.1.2 Le imprese medie

Per le imprese medie, diversamente dalle microimprese, l'informatica costituisce già un fattore decisivo dell'organizzazione aziendale. Le imprese medie dipendono spesso dal funzionamento di un'infrastruttura informatica. È ovvio quindi che aumenti anche il bisogno di sicurezza in questo ambito. La protezione tecnica contro il malware non può più bastare; si devono elaborare concetti e istruire i collaboratori. Nella maggior parte dei casi però le medie imprese sono troppo piccole per permettersi i servizi di specialisti responsabili della sicurezza dell'informazione. Pertanto non meraviglia affatto che le medie imprese ricerchino sostegno in ambito di sicurezza dell'informazione. Esse collaborano perlopiù con partner esterni di outsourcing, stipulano assicurazioni e ricercano in misura superiore alla media aiuti esterni in caso di eventi. Dato che numerose medie imprese non hanno assunto un informatico ma devono nondimeno ricorrere a

misure di protezione complesse, nel loro caso potrebbero essere utili soprattutto corsi di formazione e di perfezionamento, nonché piattaforme per lo scambio di esperienze.

5.1.3 Le grandi imprese

Le grandi imprese presentano a loro volta bisogni diversi. Esse devono adottare misure di protezione molto più ampie perché la loro informatica è la più minacciata. Le grandi imprese investono più denaro e personale, applicano misure tecniche molto più complesse e adottano più spesso piani di sicurezza. A causa della maggiore frequenza di attacchi mirati esse sono però anche esposte a minacce molto più ampie. I metodi degli hacker cambiano rapidamente, bisogna quindi essere costantemente aggiornati. Ma in questo caso anche gli specialisti e i team informatici giungono rapidamente al limite delle loro capacità.

Le grandi imprese sono pertanto prevalentemente interessate a consulenza specifiche tra specialisti. Non si tratta di questioni generali in ambito di sicurezza dell'informazione, bensì dell'attuazione pratica di misure finanziariamente e tecnicamente dispendiose. Queste imprese sono inoltre strettamente interconnesse e, spesso, interdipendenti. Oltre alla consulenza devono essere organizzati e promossi la collaborazione e lo scambio reciproco. In caso di attacchi contro la loro sicurezza dell'informazione, per le grandi imprese può essere importante anche la collaborazione con la polizia.

Le esigenze delle grandi imprese divergono quindi chiaramente da quelle delle piccole e medie imprese. I loro bisogni di consulenza specifica e di collaborazione sono però già noti da tempo e se ne è anche tenuto conto nell'offerta di una stretta collaborazione con MELANI. Per motivi di costi e di risorse una più intensa cooperazione può però essere messa a disposizione di una cerchia relativamente ristretta di grandi imprese.

5.2 Cooperazione nonostante la diversità delle esigenze: Warning, Advice and Reporting Points (WARPs) come possibile soluzione

Il secondo importante punto che emerge dal presente studio è che le imprese svizzere sarebbero disposte a una maggiore collaborazione nell'ambito della sicurezza dell'informazione. Numerose imprese affrontano con difficoltà analoghe e potrebbero approfittare di uno scambio di esperienze. Il problema a livello di attuazione della cooperazione risiede nel fatto più sopra rilevato che le diverse imprese hanno necessità diverse.

Una possibile soluzione potrebbe consistere nella creazione di Warning, Advice and Reporting Points (WARPs). Il «National Infrastructure Security Coordination Center» (NISCC) del governo britannico diffonde simili WARPs come piattaforma ideale di scambio e di collaborazione in ambito di sicurezza dell'informazione[51]. I membri dei WARPs si scambiano informazioni e lottano in comune contro le minacce alla sicurezza dell'informazione. Si possono così individuare precocemente le nuove minacce e mettere le possibili soluzioni a disposizione di tutti i membri. È decisivo il fatto che a seconda delle necessità i WARPs possono essere creati tra imprese del medesimo settore, della medesima regione o della medesima classe di dimensioni. All'interno dei WARPs collaborano imprese che hanno problemi analoghi e presentano bisogni analoghi. I risultati dello studio mostrano che le dimensioni delle imprese costituiscono uno dei principali criteri di strutturazione dei WARPs. Se infatti le grandi imprese sono soprattutto

51 http://www.niscc.gov.uk/niscc/warpInfo-en.html.

interessate a consulenze specifiche tra specialisti, nel caso delle piccole e medie imprese sussiste invece il bisogno di una consulenza generica e di uno scambio reciproco. I WARPs potrebbero pertanto essere particolarmente idonei alle medie imprese, perché mediante la cooperazione tra imprese comparabili la sicurezza dell'informazione può essere migliorata senza che ne risultino costi elevati.

Lo Stato potrebbe fornire l'impulso alla creazione di simili WARPs e coordinarli nella fase iniziale. La creazione dei WARPs potrebbe necessitare di un sostegno da parte dello Stato perché le imprese hanno tendenza a partecipare a simili organizzazioni soltanto quando la loro utilità è stata comprovata. Sarebbe inoltre importante coordinare i diversi WARPs perché tra di essi vi sarebbero interfacce che potrebbero essere sfruttate. In tal modo, mentre nel quadro di WARPs specializzati le imprese potrebbero dedicarsi alla tutela della loro attività commerciale, lo Stato, dal canto suo, promuoverebbe la sicurezza dell'intera economia tramite il coordinamento di queste diverse organizzazioni, perseguendo i propri obiettivi in materia di politica di sicurezza.

6 Bibliografia

Abele-Wigert, Isabelle e Myriam Dunn, *The International Critical Information Infrastructure Protection (CIIP) Handbook 2006. An Inventory and Analysis of Protection Policies in Twenty Countries* (Zurigo, 2006).

Bidgoli, Hossein et al. (ed.), *Handbook of Information Security Volume 1-3* (Hoboken, 2006).

Bundesamt für Sicherheit für Sicherheit in der Informationstechnik (BSI), *Die Lage der IT-Sicherheit in Deutschland 2005* (luglio 2005).
http://www.bsi.bund.de/literat/lagebericht/lagebericht2005.pdf

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), *Sicurezza dell'informazione. Situazione in Svizzera e a livello internazionale. Rapporto semestrale 2005/1* (2005).
http://www.melani.admin.ch/berichte/lageberichte/index.html?lang=de#sprungmarke0_3

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), *Sicurezza dell'informazione. Situazione in Svizzera e a livello internazionale. Rapporto semestrale 2005/2* (2006).
http://www.melani.admin.ch/berichte/lageberichte/index.html?lang=de#sprungmarke0_3

Computer Security Institute(CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005). http://www.gocsi.com

Dübendorfer, Thomas, Arno Wagner und Bernhard Plattner, *An Economic Model for Large-Scale Internet Attacks* (Studio del Computer Engineering and Networks Laboratory del PF di Zurigo, 2004).
http://www.tik.ee.ethz.ch/~ddosvax/publications/papers/WETICE-ES-duebendorfer-economic_damage_model.pdf

Eckert, Claudia, *IT-Sicherheit: Konzepte – Verfahren – Protokolle* (3ª ed. rielaborata e ampliata 3, Monaco di Baviera, Oldenbourg, 2004).

Federal Bureau of Investigation (FBI), *2005 FBI Computer Crime Survey* (2005).
http://www.fbi.gov/publications/ccs2005.pdf

Gartner Research, *Enterprises and Employees: The Growth of Distrust* (2005). Compendio dei risultati in: http://www.csoonline.com/analyst/report3317.html

Haldemann, Lukas, *Versicherung von Internet-Risiken* (lavoro di seminario al Dipartimento di informatica del PF di Zurigo, 2001).
http://www.ifi.unizh.ch/ikm/Vorlesungen/inf_recht/2001/Haldemann.pdf

KPMG, *IT-Management 2005: Standortbestimmung und Trends in der Schweizer Informatik* (Zurigo e Ginevra, 2005).

National Hi-Tech Crime Unit (nhtcu), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005).
http://www.gfknop.co.uk/content/news/news/Impact%20of%20HTC%20NOP%20Survey%202005.pdf

Sieber, Pascal, Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002 (studio su mandato del Segretariato di Stato dell'economia, Berna, 2002).

7 Allegato

Allegato 1: Composizione del campionario / Suddivisione delle imprese

- Il **complesso di base è costituito da tutte le imprese svizzere** del secondo e del terzo settore.
- Ne sono state escluse tutte le grandi imprese che fanno parte della cerchia della clientela di MELANI-Net.
- Ai fini dell'inchiesta ci si è sforzati di ottenere la partecipazione di almeno 500 imprese. La percentuale di riflusso è stata stimata nel 10 per cento delle imprese interrogate. Ne risulta un **campionario auspicato di 5 000 imprese**.

- **Criteri di differenziazione delle imprese:**

  a) **Classi di dimensioni:**
     - Imprese piccole (microimprese): 0–4 posti a tempo pieno
     - Piccole imprese: 5–9 posti a tempo pieno
     - Medie imprese: 10–49 posti a tempo pieno
     - Grandi imprese: 50–249 posti a tempo pieno
     - Grandissime imprese: oltre 250 posti a tempo pieno

  b) **Settori** secondo la nomenclatura delle attività economiche dell'Ufficio federale di statistica[52].
     - **Industria, attività manifatturiere:** unità che si occupano della trasformazione meccanica, fisica o chimica di materiali, sostanze o componenti in nuovi prodotti.
     - **Costruzioni:** lavori generali e speciali di costruzione, lavori di installazione e altri lavori di completamento degli edifici.
     - **Commercio:** vendita all'ingrosso e al dettaglio (vendita senza trasformazione) di ogni genere di beni e fornitura di servizi correlati alla vendita di merci.
     - **Alberghi e turismo:** unità che forniscono ai clienti alloggio e/o che preparano pasti, spuntini e bevande per il consumo immediato.
     - **Trasporti e comunicazioni:** attività collegate al trasporto, regolare o meno, per ferrovia, mediante condotte, su strada, per via d'acqua, via aerea, di passeggeri o merci. Attività ausiliarie quali terminal, parcheggi, centri di movimentazione e magazzinaggio di merci ecc. Attività delle poste e telecomunicazioni. Noleggio di mezzi di trasporto senza autista od operatore.
     - **Attività finanziarie:** attività di ottenimento e ridistribuzione di mezzi finanziari a fini diversi da quelli dell'assicurazione sociale obbligatoria o dei fondi pensione.
     - **Servizi alle imprese:** attività concernenti in maniera particolare il settore delle imprese. Quasi tutte le attività di questa sottosezione possono essere fornite tuttavia anche a privati, ad es. noleggio di beni personali e per la casa, attività delle banche di dati, attività legali, servizi di investigazione e vigilanza, arredamento di interni o attività fotografiche.

52 NOGA: Nomenclatura generale delle attività economiche. Maggiori informazioni su questa nomenclatura sulla homepage dell'Ufficio federale di statistica: http://www.bfs.admin.ch/bfs/portal/de/index/infothek/nomenklaturen/blank/blank/noga0/publikationen.html

- **Servizi informatici:** attività in relazione con l'hardware e il software ed elaborazione elettronica dei dati.
- **Pubblica amministrazione:** attività normalmente svolte dall'amministrazione pubblica. Lo status giuridico o istituzionale non è di per sé il fattore determinante.
- **Istruzione:** istruzione, pubblica e privata, di qualsiasi tipo e a tutti i gradi, impartita dalle varie istituzioni che compongono il sistema scolastico tradizionale, ma anche istruzione per adulti, programmi di alfabetizzazione ecc.
- **Attività dei servizi sanitari:** servizi ospedalieri, servizi degli studi medici, servizi veterinari, assistenza sociale (case per anziani, case di cura medicalizzate e istituti per adolescenti).
- **Altri servizi:** servizi che non rientrano primariamente nei servizi forniti alle imprese (p. es. cultura, sport, lavanderie, saloni di parrucchiere e istituti di bellezza ecc.).

- **Piano di campionatura:**
  Il campionario deve essere stratificato in modo che siano possibili affermazioni per le diverse classi di dimensioni e per i diversi settori. È stato pertanto scelto un approccio di campionatura disproporzionale (Quota-Random). In questo approccio i singoli strati sono sottorappresentati o sovrarappresentati; per questa ragione si è proceduto successivamente a una correzione tramite ponderazione. In numerosi settori si è reso necessario un rilevamento completo di tutte le imprese con oltre 250 collaboratori perché esistono solo poche grandi imprese.
  Gli indirizzi delle imprese sono stati richiesti all'Ufficio federale di statistica secondo il seguente piano di campionatura:

Quote prestabilite per l'ordinazione degli indirizzi

Sezioni NOGA (divisioni)	Categoria di dimensioni (Petp)		
	0-9	10-249	250+
D Produzione di merci (15-37)	330	420	250
F Edilizia (45)	300	390	RI
G Commercio (50-52)	500	400	100
H Alberghi e turismo (55)	220	320	RI
I Trasporti e trasmissione di informazioni (60-64)	200	200	RI
J Istituti di credito e assicurazioni (65-67)	120	160	RI
K Settore immobiliare, servizi alle imprese (70-74)	550	350	RI
L Pubblica amministrazione, difesa, assicurazioni sociali (75)	60	130	RI
M Educazione e istruzione (80)	140	210	RI
N Sanità, settore veterinario, settore sociale (85)	270	220	100
O Altri servizi a terzi (90-93)	310	200	RI
Total	**3'000**	**3'000**	**~1000**

Petp = posti equivalenti a tempo pieno
RI = rilevamento integrale

- È stata mantenuta una riserva di 2 000 indirizzi. Il formulario di inchiesta è stato inviato a 5 000 imprese; alcuni indirizzi non erano più attuali. Il campionario comprendeva effettivamente 4 916 imprese.

Allegato 2: Il riflusso

- 562 imprese hanno partecipato all'inchiesta; la **percentuale di riflusso** è quindi dell'**11.45 per cento**.
- Non è stata condotta un'analisi sistematica delle **imprese non partecipanti**. Come nel caso di ogni inchiesta nel cui ambito solo una parte dei destinatari compila il questionario, sussiste il pericolo che i partecipanti si distinguano dalla media in importanti settori. Si potrebbe pensare che la partecipazione all'inchiesta indichi che una determinata impresa si interessi più delle altre alla tematica della sicurezza dell'informazione. Indicazioni sui motivi della mancata partecipazione sono state fornite dalle imprese che hanno comunicato il proprio ritiro dall'inchiesta. Su **44 ritiri** la metà è dovuta all'assenza di interesse o di tempo. 8 imprese hanno comunicato di non utilizzare l'informatica, mentre altre 10 hanno indicato che non si considerano competenti per rispondere alle domande. 4 imprese non hanno voluto rispondere al questionario per motivi di sicurezza.

  Riflusso per classi di dimensioni:

Dimensioni	Numero	Precentuale
0-4	132	23.49
5-9	62	11.03
10-49	195	34.70
50-249	86	15.30
>250	87	15.48

  Riflusso per settori:

Settore	**Numero**	**Precentuale**
Industria	82	14.59
Edilizia	92	16.37
Commercio	59	10.50
Ristorazione	20	3.56
Trasporti e comunicazioni	37	6.58
Finanze	21	3.74
Servizi alle imprese	53	9.43
Servizi informatici	37	6.58
Amministrazione pubblica	42	7.47
Istruzione	14	2.49
Sanità	56	9.96
Altri servizi	49	8.72

Allegato 3: Ponderazione dei dati

- **I partecipanti all'inchiesta non costituiscono una riproduzione della realtà per quanto concerne le dimensioni e l'appartenenza settoriale delle imprese.** Nella realtà soltanto lo 0,3 per cento di tutte le imprese occupa oltre 250 collaboratori, mentre nel quadro dell'inchiesta esse rappresentano il 15 per cento dei partecipanti. A livello settoriale le imprese del settore delle costruzioni sono rappresentate in proporzione eccessiva, mentre le imprese che forniscono servizi alle imprese e quelle del settore degli alberghi e del turismo sono sottorappresentate.
- La riproduzione sproporzionata della realtà è necessaria, affinché i dati siano di volta in volta sufficienti per operare un confronto. Questo significa però che dalle affermazioni della media dei partecipanti non si possono direttamente desumere conclusioni sulla media di tutte le imprese svizzere del secondo e del terzo settore.
- Per potere nondimeno effettuare stime su tutte le imprese della Svizzera i dati devono essere ponderati.
- Effettuare una ponderazione significa **moltiplicare tutti i dati per il fattore di ponderazione w**. Tale fattore è calcolato come segue:

$$w = \frac{n_{Ri}/N_R}{n_{Si}/N_S}$$

n_{Ri}= numero di imprese della categoria i nella realtà
N_R= numero di imprese nella realtà
n_{Si}= numero di imprese della categoria i nel campionario
N_S= numero di imprese del campionario

- Complessivamente occorre distinguere tra 60 categorie (6 classi di dimensioni e 12 diversi settori). Il fattore di ponderazione w di ognuna di questa categorie può essere calcolato dividendo la sua percentuale nella realtà per la sua percentuale nel campionario.

Settore	Total (realtà)	Total (inchiesta)	Ponderazione	0-4 (r)	0-4 (i)	Pond.	5-9 (r)	5-9 (i)	Pond.
Industria	12.82	14.59	0.88	8.17	1.43	5.72	1.86	0.71	2.61
Edilizia	10.91	16.37	0.67	7.11	2.50	2.85	1.88	3.39	0.55
Commercio	22.60	10.50	2.15	17.36	3.21	5.41	3.08	1.07	2.88
Ristorazione	7.91	3.56	2.22	5.02	0.36	13.96	1.74	0.36	4.85
Trasporti e comunicazioni	3.50	6.58	0.53	2.53	1.61	1.57	0.43	0.54	0.79
Finanze	1.71	3.74	0.46	1.07	0.89	1.20	0.25	0.00	
Servizi alle imprese	19.39	9.43	2.06	16.39	3.21	5.11	1.78	1.25	1.43
Servizi informatici	3.52	6.58	0.53	2.90	3.04	0.95	0.30	0.54	0.56
Amministrazione pubblica	0.74	7.47	0.10	0.29	0.89	0.32	0.11	0.89	0.13
Istruzione	2.21	2.49	0.89	1.28	1.07	1.20	0.25	0.00	
Sanità	6.87	9.96	0.69	5.29	2.32	2.28	0.69	0.89	0.78
Altri servizi	7.83	8.73	0.90	6.64	3.04	2.18	0.69	1.25	0.55
Totale	100.00	100.00		74.06	23.49		13.08	11.03	
Settore	10-49 (r)	10-49 (i)	Pond.	50-249 (r)	50-249 (i)	Pond.	250+ (r)	250+ (i)	Pond.
Industria	2.06	4.64	0.44	0.60	3.93	0.15	0.13	3.93	0.03
Edilizia	1.68	7.32	0.23	0.22	2.32	0.10	0.02	0.89	0.02
Commercio	1.84	4.64	0.40	0.26	0.54	0.48	0.05	1.07	0.05
Ristorazione	1.03	2.14	0.48	0.10	0.36	0.28	0.01	0.18	0.05
Trasporti e comunicazioni	0.43	2.68	0.16	0.09	0.89	0.10	0.02	0.89	0.02
Finanze	0.30	0.54	0.55	0.06	0.18	0.34	0.03	2.14	0.02
Servizi alle imprese	1.05	2.32	0.45	0.14	1.79	0.08	0.02	0.89	0.02
Servizi informatici	0.27	1.96	0.14	0.04	0.36	0.11	0.01	0.71	0.01
Amministrazione pubblica	0.21	1.79	0.12	0.09	1.79	0.05	0.03	2.14	0.01
Istruzione	0.49	1.07	0.46	0.16	0.18	0.91	0.02	0.18	0.14
Sanità	0.59	2.86	0.20	0.25	1.96	0.13	0.06	1.79	0.03
Altri servizi	0.42	2.86	0.15	0.06	0.89	0.07	0.01	0.71	0.01
Totale	10.37	34.70		2.09	15.30		0.40	15.48	

Allegato 4: Procedura di ponderazione per escludere l'influsso dell'appartenenza settoriale / delle dimensioni dell'impresa

- Nel caso di alcune analisi è stato esaminato l'influsso delle dimensioni dell'impresa o dell'appartenenza settoriale. A tale scopo occorre escludere di volta in volta l'altro influsso.

  Esempio: le imprese del settore finanziario interrogate sono nella misura del 57 per cento grandi imprese con oltre 250 collaboratori. Rispetto alla percentuale di grandi imprese del campionario (16%), queste imprese sono chiaramente sovrarappresentate nel settore finanziario. Se risulta ora dall'analisi che le imprese del settore finanziario investono molto nella sicurezza dell'informatica, questa affermazione potrebbe essere una conseguenza della rappresentanza eccessiva di grandi imprese in questo settore.
- Deve pertanto essere applicato il fattore di ponderazione w_2, tramite il quale i dati sono valutati in modo tale che in tutti i settori le classi di dimensioni siano uguali e che in tutte le classi di dimensioni i settori siano rappresentati con la medesima frequenza. La formula del fattore di ponderazione w_2 è la seguente:

$$w_2 = \frac{n_i / n_{Bi}}{n_{Gi} / N} = \frac{n_i \, N}{n_{Bi} \, n_{Gi}}$$

n_i = numero di imprese della categoria i
n_{Bi} = numero di imprese del settore della categoria i
n_{Gi} = numero di imprese della classe di dimensioni della categoria i.
N = numero di imprese dell'intero campionario

Calcolo di w_2 con l'ausilio delle quote percentuali di classi di dimensioni per settore:

Settore	0-4 (S)	0-4 (M)	Pond.	5-9 (S)	5-9 (M)	Pond.	10-49 (S)	10-49 (M)	Pond.	50-249 (S)	50-249 (M)	Pond.	250+ (S)	250+ (M)	Pond.
Industria	9.76	23.57	2.41	4.88	10.89	2.23	31.71	34.82	1.10	26.83	15.19	0.57	26.83	15.52	0.58
Edilizia	15.22	23.57	1.55	20.65	10.89	0.53	44.57	34.82	0.78	14.13	15.19	1.08	5.43	15.52	2.86
Commercio	30.51	23.57	0.77	10.17	10.89	1.07	44.07	34.82	0.79	5.08	15.19	2.99	10.17	15.52	1.53
Ristorazione	10.53	23.57	2.24	10.53	10.89	1.03	63.16	34.82	0.55	10.53	15.19	1.44	5.26	15.52	2.95
Trasporti e comunicazioni	24.32	23.57	0.97	8.11	10.89	1.34	40.54	34.82	0.86	13.51	15.19	1.12	13.51	15.52	1.15
Finanze	23.81	23.57	0.99		10.89		14.29	34.82	2.44	4.76	15.19	3.19	57.14	15.52	0.27
Servizi alle imprese	33.96	23.57	0.69	13.21	10.89	0.82	24.53	34.82	1.42	18.87	15.19	0.80	9.43	15.52	1.65
Servizi informatici	45.95	23.57	0.51	8.11	10.89	1.34	29.73	34.82	1.17	5.41	15.19	2.81	10.81	15.52	1.44
Amministrazione pubblica	11.90	23.57	1.98	11.90	10.89	0.92	23.81	34.82	1.46	23.81	15.19	0.64	28.57	15.52	0.54
Istruzione	42.86	23.57	0.55		10.89		42.86	34.82	0.81	7.14	15.19	2.13	7.14	15.52	2.17
Sanità	23.64	23.57	1.00	9.09	10.89	1.20	29.09	34.82	1.20	20.00	15.19	0.76	18.18	15.52	0.85
Altri servizi	34.69	23.57	0.68	14.29	10.89	0.76	32.65	34.82	1.07	10.20	15.19	1.49	8.16	15.52	1.90

(S): quota percentuale nel singolo settore
(M): quota percentuale media

Allegato 5: Questionario

- L'inchiesta è stata effettuata online. Le imprese interrogate hanno ricevuto un invito (per lettera o per e-mail), contenente una password. In tal modo esse potevano effettuare il login sulla pagina www.unipark.de/informatiksicherheit.

- L'inchiesta è durata dal 15.03.06 al 13.04.06.

Benvenuti all'inchiesta online

«Sicurezza informatica in Svizzera»

L'inchiesta è effettuata dal Centro di ricerca per la politica di sicurezza del Politecnico federale di Zurigo (PFZ).

Informazioni per la compilazione del questionario::
Il questionario è rivolto alle imprese e alle autorità.
A titolo di semplificazione le domande sono rivolte a tutti i partecipanti come se fossero ditte o imprese.
Tutte le indicazioni fornite sono trattate in modo strettamente confidenziale e anonimo.
Per ulteriori domande rivolgetevi a:
suter@sipo.gess.ethz.ch
Vogliate p.f. compilare il questionario entro il 31 marzo 2006.

In quale settore opera la vostra impresa (attività principale)?
Selezionate per favore un solo settore.

- ○ Industria, produzione di merci
- ○ Edilizia
- ○ Commercio (generi alimentari e oggetti d'uso)
- ○ Industria alberghiera, ristorazione
- ○ Trasporti e trasmissione di informazioni
- ○ Credito e assicurazione
- ○ Immobili
- ○ Prestazioni informatiche
- ○ Altre prestazioni per le imprese
- ○ Educazione
- ○ Sanità e opere sociali
- ○ Amministrazione pubblica
- ○ Altro

Quale è il numero di persone occupate nella vostra ditta?
Compresi gli apprendisti; il personale occupato a tempo parziale va convertito in personale a tempo pieno; se del caso considerate i collaboratori all'estero.

- ○ 0-4
- ○ 5-9
- ○ 10-49
- ○ 50-249
- ○ plus de 250

Quale cifra d'affari ha realizzato la vostra impresa nel 2005?
Indicazioni in franchi svizzeri

- ○ Meno di 1 milione
- ○ 1-4,9 milioni
- ○ 5-9,9 milioni
- ○ 10-99 milioni
- ○ Oltre 100 milioni
- ○ Non so

Quale è la percentuale di collaboratori della vostra ditta che utilizza i seguenti strumenti ausiliari per svolgere il proprio lavoro:

	0%	1-20%	21-40%	41-60%	61-80%	81-100%	Non so
Personal Computer (PC)	○	○	○	○	○	○	○
Laptop	○	○	○	○	○	○	○
Palmare (organizer, PDA)	○	○	○	○	○	○	○
Telefono cellulare	○	○	○	○	○	○	○
E-mail	○	○	○	○	○	○	○
Internet	○	○	○	○	○	○	○

I vostri collaboratori possono accedere da casa alla vostra rete aziendale?

- ○ Sì, illimitatamente
- ○ Sì, a determinate condizioni
- ○ No
- ○ Non so

Quale tipo di collegamento a Internet utilizza la vostra impresa?
Sono possibili più risposte.

- ☐ Modem
- ☐ ISDN
- ☐ DSL (xDSL, ADSL, SDSL ecc.) < 2Mb/sec
- ☐ Modem via cavo o altri collegamenti a banda larga
- ☐ Altro

La vostra ditta utilizza reti wireless?

- ○ Si
- ○ No
- ○ Non so

La vostra ditta è presente su Internet con una homepage?

- ○ Si
- ○ No
- ○ Non so

Quali offerte presenta la homepage?
Sono possibili più risposte.

- ☐ Informazioni sulla vostra ditta (indirizzi, scopo aziendale ecc.)
- ☐ Informazioni sui vostri prodotti (pubblicità)
- ☐ Vendita di prodotti senza traffico online dei pagamenti
- ☐ Vendita di prodotti compreso il traffico online dei pagamenti
- ☐ Altro

La vostra ditta utilizza le seguenti possibilità di Internet?

	Si	No	Non so
Ricerca di informazioni	○	○	○
Formazione perfezionamento professionale	○	○	○
Forum di discussione	○	○	○
Acquisto di prodotti e di prestazioni di servizi	○	○	○

Valutate per favore l'importanza della struttura informatica per la vostra impresa.

meno importante ○ ○ ○ ○ ○ molto importante

Quale è stata l'evoluzione della percentuale di investimenti nell'infrastruttura informatica nel corso degli ultimi cinque anni?

diminuzione	rimasto stabile	aumento	Non so
○	○	○	○

Nel corso del 2005 avete constatato uno dei seguenti attacchi contro la sicurezza informatica della vostra ditta?

- ☐ Virus, vermi, cavalli di Troia
- ☐ Spyware
- ☐ Attacchi contro la disponibilità (Denial of Service, DoS)
- ☐ Penetrazione nel sistema (hacking)
- ☐ Furto di dati
- ☐ Furto di laptop o di altro materiale informatico
- ☐ Uso abusivo delle reti senza fili
- ☐ Deturpamento della homepage (defacement)
- ☐ Altro
- ☐ Non abbiamo constatato un attacco

Da dove provenivano questi attacchi?

- ○ Gli attacchi provenivano dall'esterno
- ○ Gli attacchi sono stati originati da uno dei collaboratori
- ○ Sono stati constatati attacchi sia dall'esterno che dall'interno

Di quante persone è composto il team che si occupa della sicurezza informatica della vostra impresa?
Convertite il personale a tempo parziale in personale a tempo pieno.

- ○ Nessuna
- ○ 0-1
- ○ 2-5
- ○ 6-10
- ○ Oltre 10

Quale è la formazione del capo di questo gruppo?

- ○ Informatico con diploma universitario
- ○ Apprendistato compiuto di informatico
- ○ Certificato federale di informatico
- ○ Perfezionamento professionale accessorio nel settore dell'informatica
- ○ Altra formazione

Quali sono state nel 2005 le spese complessive per la sicurezza informatica?
Indicazioni in franchi svizzeri. Considerate le spese di personale e di struttura.

- ○ 0-5'000
- ○ 5'001-20'000
- ○ 20'001-100'000
- ○ 100'000 oppure oltre
- ○ Non so

Nel 2006 la vostra ditta spenderà probabilmente di più o di meno per il settore della sicurezza informatica?

- ○ Di più
- ○ Di meno
- ○ Altrettanto
- ○ Non so

Nel settore della sicurezza informatica quale percentuale dei mezzi viene delegata ad altre ditte (outsourcing)?

0%	1-20%	21-40%	41-60%	61-80%	81-100%	Non so
○	○	○	○	○	○	○

In che misura condividete queste affermazioni: "In ambito di sicurezza informatica la mia impresa investe mezzi sufficienti ...

	Corrisponde al vero	Corrisponde relativamente al vero	Né sì né no	Non corrisponde pienamente	Non corrisponde affatto	Non so
...nei meccanismi tecnici di protezione."	○	○	○	○	○	○
...nel perfezionamento professionale dei responsabili IT."	○	○	○	○	○	○
...nel perfezionamento professionale di collaboratori."	○	○	○	○	○	○

Quali meccanismi di protezione utilizzate per garantire la sicurezza dei vostri sistemi informatici?
Sono possibili più risposte.

- [ ] Programmi antivirus
- [ ] Firewall
- [ ] Cifratura
- [ ] Programmi anti-spyware
- [ ] Intrusion Detection
- [ ] Formazione dei collaboratori in ambito di sicurezza informatica
- [ ] Biometria
- [ ] Altro
- [ ] Nessuno

Effettuate regolarmente analisi della sicurezza informatica?

- ○ Sì, a livello aziendale interno
- ○ Sì, da parte di una ditta esterna
- ○ Non ancora, ma sono pianificate
- ○ No
- ○ Non so

Quale dei seguenti concetti applicate?
Sono possibili più risposte.

- [ ] Concetto di backup
- [ ] Concetto di sicurezza (security policy)
- [ ] Gestione dell'aggiornamento (vulnerability management)
- [ ] Gestione degli eventi (incident response management)
- [ ] Altro
- [ ] Nessuno

La vostra ditta dispone di un'assicurazione per coprire i danni eventuali alla sua struttura informatica (hardware, software, perdita di dati)?

- ○ Si
- ○ No
- ○ Non so

Quali sono i motivi per i quali la vostra ditta non dispone di un'assicurazione contro simili danni?
Sono possibili più risposte.

- [ ] Non vale la pena
- [ ] Non sapevo che sono possibili simili assicurazioni
- [ ] Non sono disponibili mezzi finanziari per questi scopo
- [ ] Le offerte delle assicurazioni sono insufficienti
- [ ] Altro

Ricercate (voi o la vostra ditta) aiuti esterni in caso di problemi di sicurezza informatica?

- ○ Si
- ○ No
- ○ Non so

Dove?
Sono possibili più risposte.

- ☐ Produttore di software
- ☐ Fornitore (provider) di servizi (ISP)
- ☐ Colleghi /conoscenti di altre ditte
- ☐ Internet (Web, forum su Internet)
- ☐ Altro

La vostra ditta fa intervenire la polizia se constata un accesso non autorizzato al sistema informatico?

- ○ Si
- ○ No
- ○ Non so

Quali motivi vi hanno indotto a non comunicare questi eventi alla polizia?
Sono possibili più risposte.

- ☐ Non sapevo che la polizia si interessasse simili eventi
- ☐ La polizia non offre possibilità di notifica si simili eventi
- ☐ Le misure autonome sono più efficienti
- ☐ Temo le conseguenze negative per l'immagine della ditta
- ☐ Gli eventi appaino poco gravi

Sareste disposti a utilizzare i servizi di un servizio di assistenza (help desk) che vi fornisca consulenza su questioni di sicurezza informatica?

- ○ Sì, in ogni caso
- ○ Sì, ma soltanto se viene gestito a prescindere dai produttori di software
- ○ No

Un simile helpdesk (servizio di consulenza) potrebbe offrire diverse prestazioni di servizi. Quali prestazioni di servizi vi sarebbero di ausilio?

	utile	non utile
Consulenza telefonica	○	○
Consulenza tramite e-mail o ticket	○	○
Consulenza personale sul posto	○	○

Anche lo scambio di esperienze e di conoscenze con colleghi che esercitano la stessa professione può costituire un'utile fonte di informazione. A quale tipo di scambio sareste disposti a partecipare?

	Parteciperò sicuramente	Parteciperò probabilmente	Non parteciperò probabilmente	Non parteciperò sicuramente
Scambio anonimo tramite forum su Internet	○	○	○	○
Scambio tramite contatti personali	○	○	○	○
Nell'ambito di workshop organizzati dalle corrispondenti ditte di software	○	○	○	○
Nell'ambito di workshop organizzati da terzi indipendenti	○	○	○	○

Ulteriori servizi e documenti potrebbero aiutarvi a migliorare la sicurezza informatica. Valutate l'utilità delle seguenti offerte.
1 significa «poco utile»; 5 significa «molto utile».

	1	2	3	4	5
Manuale sulla procedura da seguire per sporgere querela penale	○	○	○	○	○
Materiale di base per la formazione , rispettivamente per la sensibilizzazione dei collaboratori	○	○	○	○	○
Raccomandazioni tratte dalla "Best Practices" (p. es. ISO 17799)	○	○	○	○	○
Assistenza per l'applicazione di "Best Practices" (p. es. ISO 17799)	○	○	○	○	○
Manuale per affrontare gli eventi	○	○	○	○	○

A parere vostro chi sarebbe maggiormente idoneo a fornire i servizi menzionati?

- ○ Imprese di software
- ○ Organizzazioni statali
- ○ Associazioni settoriali
- ○ Organizzazioni appositamente istituite
- ○ Imprese di consulenza

La vostra ditta sarebbe disposta a partecipare al finanziamento dei costi di simili servizi?

- ○ Sì, fino a un massimo di CHF 500 all'anno
- ○ Sì, fino a un massimo di CHF 2'000 all'anno
- ○ No
- ○ Non so

Conoscete «MELANI», la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione della Confederazione?

- ○ Si
- ○ No

In che misura MELANI può essere di ausilio per migliorare la sicurezza dei vostri sistemi informatici?

poco utile ○ ○ ○ ○ ○ molto utile

Le seguenti prestazioni di servizi di MELANI vi sono utili?

	Si	No	Non so
Avvertimenti (newsticker)	○	○	○
Moduli di annuncio di eventi	○	○	○
Indicazioni generali sui pericoli e le modalità di protezione dei siatemi di informazione	○	○	○
Dimostrazioni e programmi didattici per i vostri collaboratori	○	○	○
Liste di controllo e guide per i vostri collaboratori	○	○	○
Rapporti sulle principali tendenze e evoluzioni della sicurezza informatica	○	○	○

Autore

Manuel Suter, lic. phil. I, ricercatore presso il Center for Security Studies (CSS) dall'ETH di Zurigo e un membro del team di Crisis and Risk Network (CRN)

Responsabili del progetto

Dr. Myriam Dunn, principale del New Risk Research Unit del Center for Security Studies (CSS) dell'ETH di Zurigo e coordina il Crisis and Risk Network (CRN)

Dr. Victor Mauer, sostituto direttore del Center for Security Studies (CSS) dell'ETH di Zurigo

CSS
An ETH Center

Il Servizio di ricerca per la politica di sicurezza (Center for Security Studies, CSS) del Politecnico federale di Zurigo è stato istituito nel 1986 e si occupa di politica di sicurezza svizzera e internazionale nel campo della formazione, della ricerca e dei servizi. I temi principali dell'attività di ricerca sono: nuove minacce, politica di sicurezza europea e transatlantica, strategia e dottrina, disgregazione e costruzione di Stati e politica estera e di sicurezza della Svizzera. Il Servizio di ricerca per la politica di sicurezza dirige il Network di relazioni internazionali e sicurezza (International Relations and Security Network, ISN). È in contatto con numerose organizzazioni partner nazionali e internazionali e fa parte del Centro per gli studi comparativi e internazionali (Center for Comparative and International Studies, CIS) del Politecnico federale e dell'università di Zurigo.