

Scuola Universitaria Professionale
della Svizzera Italiana

SUPSI

Dipartimento
Tecnologie
Innovative

Sicurezza informatica e utilizzo dei computer in azienda

Un'indagine nella realtà della Svizzera italiana

Aprile 2007

silvanomarioni

Indice

1	Introduzione	3
2	Caratteristiche dell'inchiesta.....	4
2.1	Presentazione	4
2.2	Modalità dell'inchiesta	5
2.3	Ringraziamenti	5
3	Risultati dell'inchiesta	6
3.1	Settori di attività.....	6
3.2	Dimensioni dell'azienda.....	8
3.3	Uso di Internet.....	10
3.4	Caratteristiche dei dati aziendali.....	14
3.5	Aspetti organizzativi	18
3.6	Aspetti tecnici	23
4	Considerazioni finali.....	25
5	Strumento di analisi dinamica dei dati.....	27
6	Glossario.....	28
7	Riferimenti.....	29
8	Appendice – Formulario di inchiesta.....	30

Questo documento è scaricabile da Internet all'indirizzo isi.dti.supsi.ch/rapporto_inchiesta.pdf

SUPSI – Dipartimento Tecnologie Innovative
Galleria 2
CH-6928 Manno
Svizzera
Tel. +41 58 666 65 11
Fax. +41 58 666 65 71
www.dti.supsi.ch
dti@supsi.ch

Silvano Marioni
www.marioni.org

1 Introduzione

Un cyberattacco lo si può scomporre in quattro concetti fondamentali: la vulnerabilità (quindi il punto debole di un sistema), la minaccia (ovvero se esistono una o più vulnerabilità che possono compromettere un sistema), il rischio (che designa la probabilità che una minaccia produca un evento di danno) e l'attacco.

Dall'inchiesta condotta dal Dipartimento Tecnologie Innovative della SUPSI emerge che le imprese della Svizzera italiana hanno preso in considerazione la vulnerabilità unicamente sotto il profilo tecnico, tralasciando altri aspetti, primo tra tutti quello legato al fattore umano. Sono tre i dati principali che emergono in questo senso: il 77% dei PC presenti nelle aziende sono collegati a Internet, nel 95% dei casi, tramite un collegamento diretto; complessivamente oltre il 90% delle informazioni presenti sui PC e sui server aziendali sono considerate critiche; mediamente in più del 50% delle aziende i dipendenti hanno delle competenze nell'uso del PC e di Internet normali, sufficienti a svolgere il lavoro quotidiano. Come detto le vulnerabilità non sono costituite unicamente da fattori tecnici, ma si basano su differenti aspetti. Nello specifico un computer con dati sensibili, collegato alla grande rete e lasciato nelle mani di persone con conoscenze di base (o forse nulle) di sicurezza. Sebbene da un lato gli amministratori di sistema abbiano implementato *firewall* e antivirus, dall'altro i dipendenti possono usare la posta elettronica per scopi privati, *chattare* con persone esterne all'azienda e consultano siti al di fuori delle esigenze di lavoro, tutte e tre operazioni potenzialmente a rischio per quanto attiene alla possibile contaminazione di un sistema.

Pur non essendo avvertito il rischio è presente. Sfogliando i rapporti semestrali della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ci si rende conto di ciò che accade sul territorio svizzero. E quando gli attacchi sono sempre più sofisticati, i soli accorgimenti tecnici non sono più sufficienti a proteggere una rete aziendale, specialmente ora che il cybercrimine è divenuto territorio di organizzazioni criminali con strutture e finanziamenti importanti. Non sono i *malware* conosciuti dagli antivirus e dai *firewall* a preoccupare, ma piuttosto gli attacchi mirati, con codice appositamente scritto per infiltrare un determinato sistema tramite un *webmail* consultato da un dipendente o una sessione di *chat* durante le ore di lavoro, utilizzando comportamenti studiati grazie anche a tecniche di *social engineering*. È dunque la prevenzione la parola chiave in questo momento di forte innovazione, dove vi è uno sfruttamento intensivo del PC per bisogni di comunicazione e dove l'utente è sempre più coinvolto nelle dinamiche di produzione con le nuove applicazioni sviluppatasi attorno al concetto di Web 2.0. Un segnale incoraggiante in questo senso ci viene dalla REMP, l'istituto di ricerche e studi dei media pubblicitari, che indica che la popolazione svizzera utilizza Internet maggiormente da casa piuttosto che dal posto di lavoro, una tendenza in atto dal 2005. Sono forse le restrizioni degli amministratori di sistema che hanno aiutato a mutare un comportamento potenzialmente pericoloso. Non che l'utilizzo di Internet debba venir proibito in azienda, ma esso deve essere rigorosamente strutturato. L'utente, anche quello con i diritti più limitati, deve venir incluso in una politica di prevenzione e di educazione all'utilizzo degli strumenti tecnologici.

Grazie all'inchiesta della SUPSI ora vi sono dati concreti che aiuteranno a riflettere su tali comportamenti, un contributo prezioso per rivedere le strategie di sensibilizzazione e informazione nell'ambito della sicurezza informatica.

Mauro Vignati

Vice responsabile sezione MELANI/Cybercrime

Ufficio federale di Polizia, Berna

2 Caratteristiche dell'inchiesta

2.1 Presentazione

Cresce la consapevolezza che la sicurezza informatica non è solo un problema tecnico, ma anche un argomento che va affrontato a livello organizzativo.

Le soluzioni tecniche sono importanti per garantire la riservatezza, l'integrità e la disponibilità dei dati aziendali, ma da sole non proteggono completamente dai diversi e purtroppo sempre nuovi rischi informatici. Per una protezione più efficace delle attività aziendali sono necessarie due pratiche fondamentali. La definizione di regole per il comportamento sia nelle attività quotidiane che nelle situazioni a rischio e la sensibilizzazione di tutto il personale ai nuovi pericoli informatici, valorizzandolo come strumento attivo di protezione.

Ma che cosa fanno le aziende della Svizzera italiana per la protezione dei loro dati aziendali e dei loro sistemi informativi?

Per approfondire questo argomento il Dipartimento Tecnologie Innovative della SUPSI ha promosso un'inchiesta sulla sicurezza dei dati aziendali e dei sistemi informativi nelle piccole e medie aziende della Svizzera italiana. Diversamente da altre inchieste, non si occupa solo di censire rischi informatici e contromisure tecniche, ma vuole esaminare i comportamenti relativi alla sicurezza informatica con l'intento di stimolare delle riflessioni utili al confronto.

L'inchiesta esamina nella prima parte le tipologie di aziende, analizzandole secondo il loro settore di attività e la loro dimensione.

Nella seconda parte viene esaminato l'utilizzo di Internet, per valutare gli atteggiamenti nei confronti di un'area che presenta significativi problemi di sicurezza. Segue un'analisi dei dati aziendali e di quanto vengono considerati importanti dall'azienda. Da ultimo, sono esaminati gli aspetti organizzativi, gli aspetti tecnici e le misure di protezione utilizzate per la sicurezza informatica.

L'invito a partecipare all'inchiesta è stato fatto utilizzando l'indirizzario SUPSI e quelli degli enti, istituti e associazioni di categoria che hanno collaborato. Sono state contattate aziende diverse per dimensione e settore di attività, invitandole a fornire le informazioni sulla loro struttura e sui loro comportamenti, per quanto concerne la sicurezza informatica.

Non è stata fatta alcuna ponderazione dei dati per riallineare i risultati con la distribuzione reale delle aziende nella società, ma si sono considerati i tassi di risposta come dati oggettivi, anche se disomogenei, per valutare l'importanza che viene data nei vari settori economici alla sicurezza informatica.

D'altra parte la sicurezza informatica non è una disciplina scientifica e sistematica ma fonda le sue basi su differenti materie quali naturalmente l'informatica ma anche il management, il diritto e la psicologia. L'insieme di queste competenze differenti permette di definire una visione d'insieme da cui derivare i comportamenti di sicurezza adeguati.

I risultati dell'inchiesta e il tasso di partecipazione mostrano quale sia il valore dato alla sicurezza informatica nelle piccole e medie aziende e nei vari settori di attività e soprattutto quanto sia alto l'interesse a confrontarsi con gli altri su questo argomento. Un tema di cui si sente molto parlare, ma di cui nella realtà pratica si conosce poco.

Silvano Marioni, CISSP

2.2 Modalità dell'inchiesta

L'inchiesta ha raccolto le informazioni sui comportamenti delle aziende rispetto alla sicurezza informatica con un formulario di 19 domande.

Durante i mesi di settembre, ottobre e novembre 2006, è stato possibile partecipare all'inchiesta scaricando il formulario da compilare e rispedendolo alla SUPSI, oppure rispondendo direttamente tramite Internet alle domande.

L'invito a partecipare è stato inviato tramite posta elettronica ai nominativi presenti nell'indirizzario SUPSI e negli indirizzari di enti, istituti e associazioni di categoria che hanno collaborato all'inchiesta per un totale di circa 2500 aziende nella Svizzera Italiana.

L'invito è stato inoltre pubblicato su newsletter, organi sociali e siti Internet di alcune delle associazioni di categoria citate sopra.

Le risposte pervenute sono state 355 con un tasso di risposta percentuale intorno al 14% che può essere considerato buono per il tipo di inchiesta. Di queste 257 hanno risposto direttamente tramite Internet mentre 98 hanno risposto utilizzando il formulario cartaceo.

Le risposte anonime sono state 39 mentre 316 partecipanti hanno ritenuto utile lasciare i propri nominativi

2.3 Ringraziamenti

Si ringraziano i seguenti enti, istituti e associazioni di categoria per la collaborazione fornita nel promuovere l'inchiesta:

- Associazione fabbricanti ramo abbigliamento del Cantone Ticino
- Associazione Industrie Ticinesi
- Associazione installatori elettricisti ticinesi
- Centro Studi Bancari
- Camera di commercio, dell'industria e dell'artigianato del Cantone Ticino
- CLUSIS, Associazione svizzera della sicurezza dei sistemi d'informazione
- Dauf SA
- Istituto di formazione delle professioni fiduciarie
- Ordine degli Avvocati del Canton Ticino
- Ordine dei medici del Canton Ticino
- Ordine dei notai del Cantone Ticino
- Sezione degli enti locali del Cantone Ticino
- Società Svizzera Impresari Costruttori, Sezione Ticino
- Unione professionale svizzera dell'automobile, Sezione Ticino

3 Risultati dell'inchiesta

3.1 Settori di attività

La suddivisione nei settori di attività è stata definita basandosi sulla criticità delle informazioni trattate e sulle necessità di sicurezza informatica. Non è stata fatta la suddivisione dettagliata secondo criteri merceologici, ma è stato tenuto in considerazione quanto è importante la continuità del servizio, l'integrità e la riservatezza dei dati all'interno del settore di attività.

Settori di attività contemplati nell'inchiesta:

- Commercio
attività commerciali, garages
- Enti pubblici
amministrazioni comunali, scuole, radio televisioni pubbliche, posta
- Produzione
aziende manifatturiere nei vari settori merceologici
- Sanità e salute
ospedali, studi medici, farmacie, società farmaceutiche
- Servizi finanziari
banche, società fiduciarie
- Settore legale
studi legali, avvocati, notai
- Diversi

Sulla base delle risposte ottenute per il settore "Diversi", si è ritenuto utile creare tre nuove categorie di attività:

- Edilizia e costruzioni
studi di ingegneria e architettura, società di costruzioni, impianti elettrici e idraulici
- Informatica e comunicazione
rivenditori di hardware e software, società di sviluppo software
- Servizi logistici e altro
società di servizi e logistica, diversi

Domanda 1. Quale è il vostro settore di attività?

Le risposte alla domanda relativa al settore di attività sono state le seguenti:

- Commercio, 48 risposte (con prevalenza di garages)
- Enti pubblici, 99 risposte (con prevalenza di amministrazioni comunali)
- Edilizia e costruzioni, 19 risposte
- Informatica e comunicazione, 32 risposte
- Servizi logistici e altro, 17 risposte
- Produzione, 40 risposte
- Sanità e salute, 25 risposte (con prevalenza di farmacie)
- Servizi finanziari, 34 risposte
- Settore legale, 41 risposte

Il grafico in percentuale relativo alle risposte è il seguente:

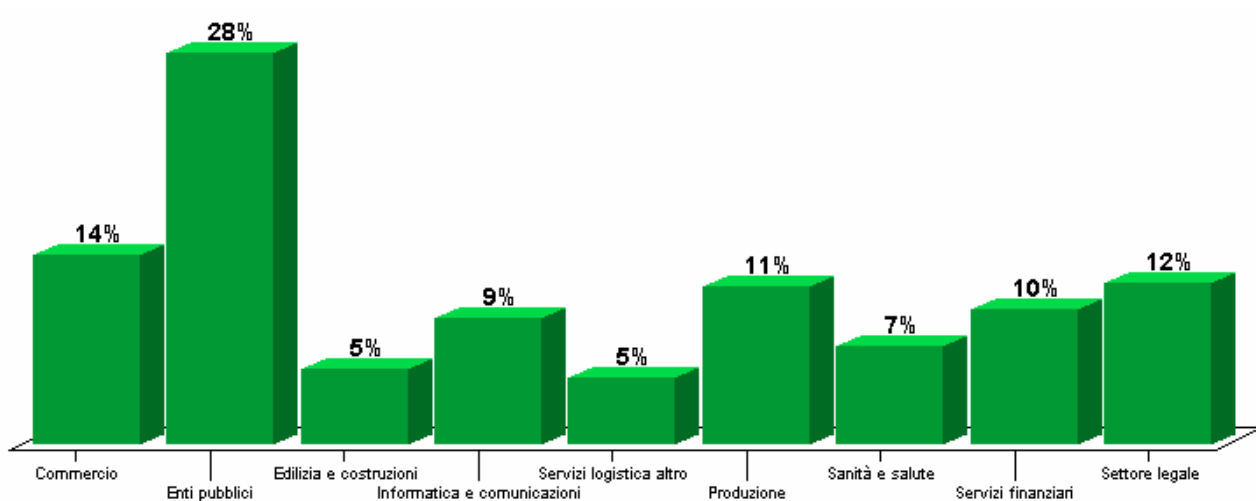


Figura 1: percentuale di aziende per settore di attività

I risultati dell'inchiesta hanno mostrato come il settore più rappresentato sia quello "Enti pubblici" con quasi un terzo delle risposte. Seguono con risposte sopra il 10% i settori "Commercio", "Settore legale" e "Produzione".

3.2 Dimensioni dell'azienda

Domanda 2. Quanti PC sono presenti nella vostra azienda?

La dimensione dell'azienda è stata censita in base al numero di PC. In alcuni casi questo potrebbe non corrispondere con la dimensione reale dell'azienda per numero di dipendenti. Tuttavia questo riesce a posizionarla rispetto alle sue potenzialità di trattamento informatico dei dati e di conseguenza alle sue esigenze di sicurezza informatica.

Le risposte per dimensione delle aziende sono state le seguenti

- 112 risposte da aziende con meno di 5 PC
- 131 risposte da aziende con dotazione tra 5 e 20 PC,
- 48 risposte da aziende con dotazione tra 20 e 100 PC,
- 64 risposte da aziende con più di cento PC,

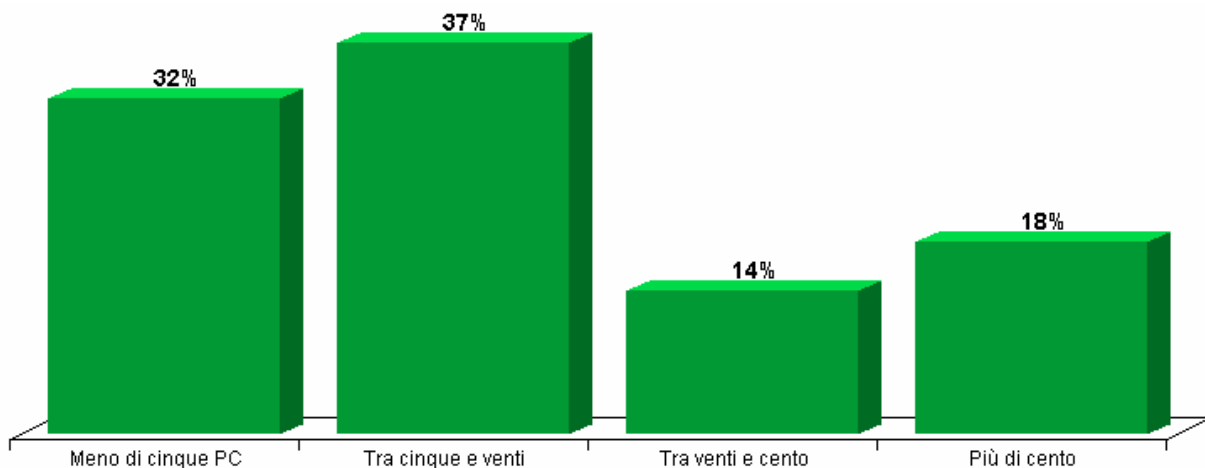


Figura 2: percentuale di aziende per numero di PC

In alcuni settori di attività, come ad esempio “Servizi finanziari” sono presenti aziende con un numero elevato di PC mentre in altri settori quali “Enti pubblici” o “Settore legale” sono caratterizzati prevalentemente da aziende con un numero di PC inferiore a 20.

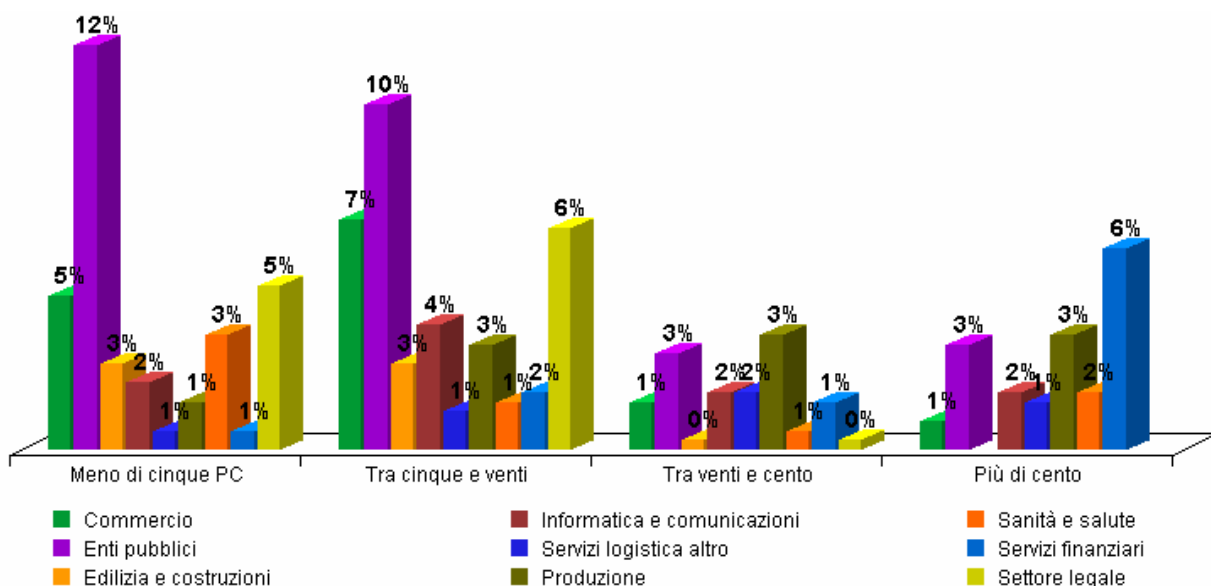


Figura 3: percentuale di aziende per numero di PC suddivisa per settore di attività

Domanda 3. Quanti server centrali sono presenti nella vostra azienda?

Anche il numero di server centrali, in rapporto con il numero dei PC, fornisce alcune informazioni aggiuntive riguardo alle dimensioni delle aziende. C'è una parziale corrispondenza tra il numero di aziende con più di 5 server (19.7%) e il numero di aziende con più di 100 PC (18%) mentre il numero delle aziende senza server (19.2%) corrisponde circa 2/3 delle aziende con meno di 5 PC (31.5%).

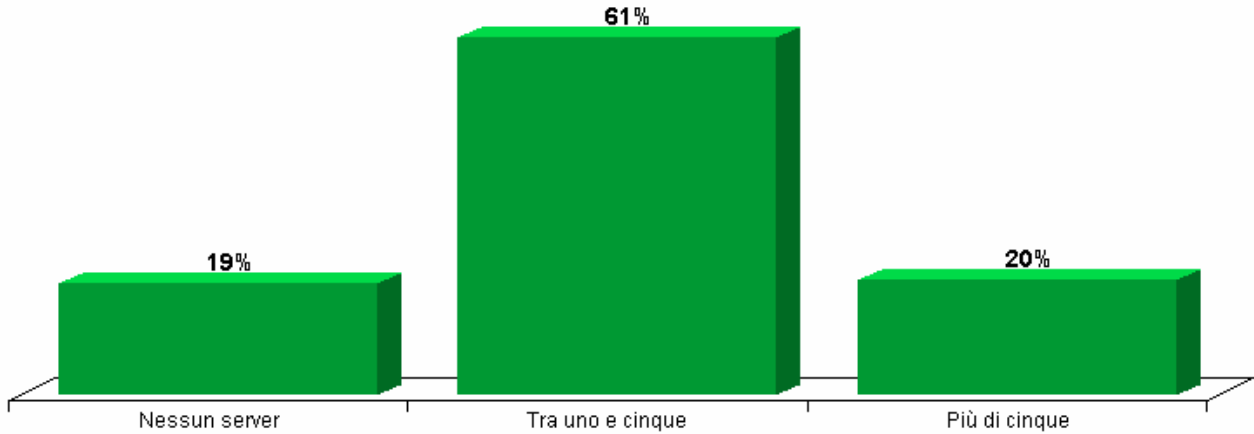


Figura 4: percentuale di aziende per numero di server centrali

3.3 Uso di Internet

Domanda 4. Esiste un collegamento Internet in azienda

Quasi tutte le risposte (99%) hanno mostrato l'esistenza di un collegamento Internet che nel 95% dei casi è diretto (ADSL, linea affittata, ecc.) e nel 4% via modem. Questo mostra come oggi Internet sia diventato uno strumento di lavoro indispensabile per aziende di ogni dimensione e di ogni settore di attività.

Domanda 5. Tutti i PC aziendali hanno accesso a Internet?

Il 77% delle aziende che hanno risposto ha indicato che tutti i PC aziendali hanno accesso a Internet. La ripartizione dei PC che possono accedere a Internet è differente a secondo dei settori di attività. Il collegamento di tutti i PC ad Internet è presente prevalentemente nelle aziende con meno di 20 PC mentre tra le aziende con oltre 20 PC è presente una percentuale maggiore di aziende che non ha tutti i PC collegati ad Internet.

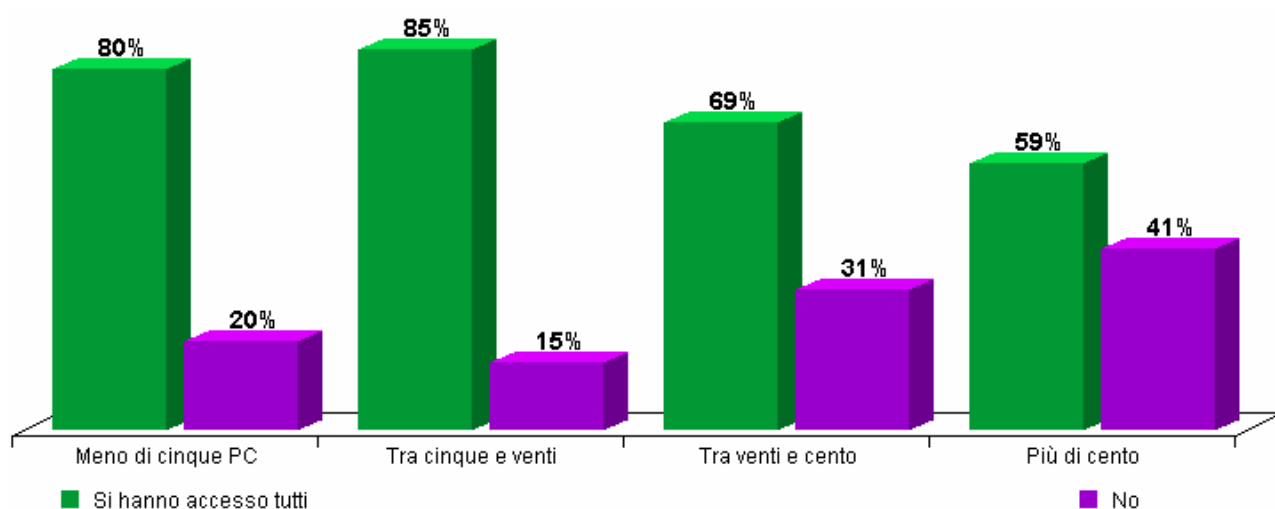


Figura 4: percentuale di aziende per numero di PC con accesso a Internet

Nel settore della “Produzione” solo il 50% delle aziende ha tutti i PC connessi a Internet mentre questa percentuale sale al 97% nel settore “Informatica e comunicazioni”.

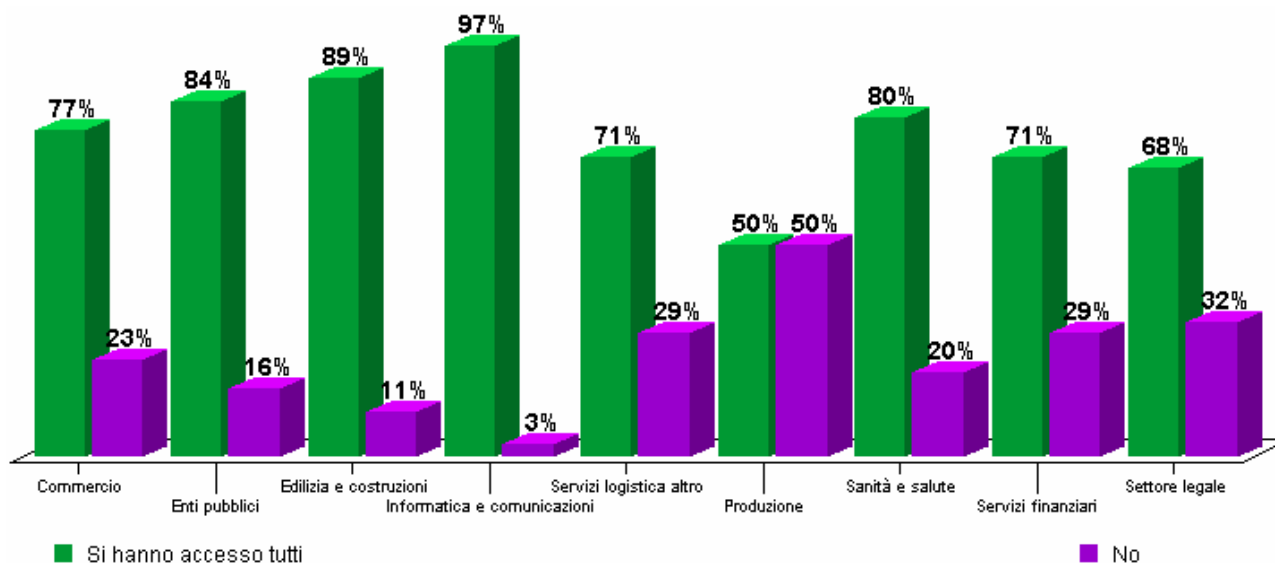


Figura 5: percentuale di aziende per numero di PC con accesso a Internet suddivisa per settore di attività

La mancata connessione a Internet non esclude che si permetta comunque ai propri dipendenti di accedervi con tecniche di disaccoppiamento dalla rete locale aziendale quali l'utilizzo di Terminal Server. Nel caso del settore "Produzione" è probabile una presenza di PC utilizzati per le attività produttive e che non hanno quindi necessità di un collegamento a Internet.

Domanda 6a. In che misura viene utilizzata la rete Internet in azienda per la posta elettronica?

Per quanto riguarda l'utilizzo della rete Internet per la comunicazione tramite posta elettronica notiamo che la maggior parte delle aziende che fa un utilizzo intensivo della posta elettronica è compresa nel settore "Informatica e comunicazione", "Servizi logistica e altro" e nei "Servizi finanziari". Seguono i settori della "Produzione" e "Sanità e salute" mentre in tutti gli altri settori solo la metà delle aziende fa un uso importante della posta elettronica.

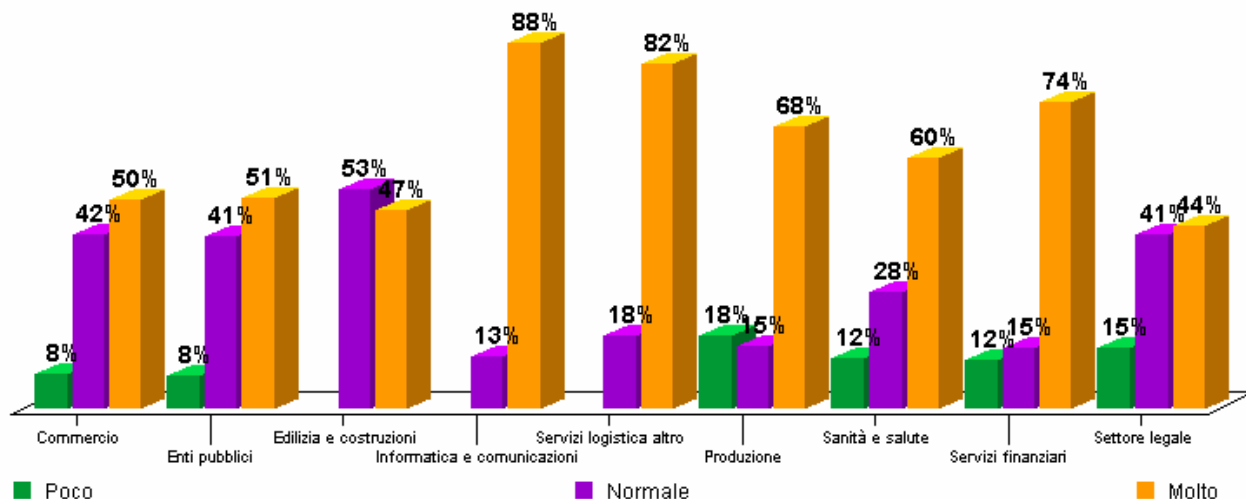


Figura 6: percentuale di utilizzo della rete Internet per la posta elettronica suddivisa per settore di attività

Si può notare che l'utilizzo della posta elettronica è maggiore nelle aziende con un elevato numero dei PC.

Utilizzo della posta elettronica	Meno di cinque PC	Tra cinque e venti PC	Tra venti e cento PC	Più di cento PC
	%	%	%	%
Poco	12.50	6.87	8.33	7.81
Normale	48.21	32.06	18.75	12.50
Molto	39.29	61.07	72.92	79.69

Figura 7: percentuale di utilizzo della rete Internet per la posta elettronica suddivisa per dimensione

Chi fa un utilizzo intensivo della posta elettronica aggiorna con maggior frequenza l'antivirus e il sistema operativo

Aggiornamento Antivirus e SO	Poco	%	Normale	%	Molto	%
	Regolarmente	28	87.50	105	92.92	199
Ogni tanto	3	9.38	8	7.08	11	5.24
Mai	1	3.13	0	0.00	0	0.00
Totale calcolato	32	100.00	113	100.00	210	100.00

Figura 8: valore e percentuale della frequenza di aggiornamento dell'antivirus e del sistema operativo suddiviso per utilizzo della rete Internet per la posta elettronica

Domanda 6b. In che misura viene utilizzata la rete Internet per attività amministrative e commerciali

Per quanto riguarda l'utilizzo di Internet per attività amministrative e commerciali notiamo che è usato soprattutto nelle aziende dei settori "Commercio", "Informatica e comunicazione", "Produzione" e "Sanità e salute". Si fa un uso più limitato nei settori "Enti pubblici", "Settore legale" e "Servizi logistica altro"

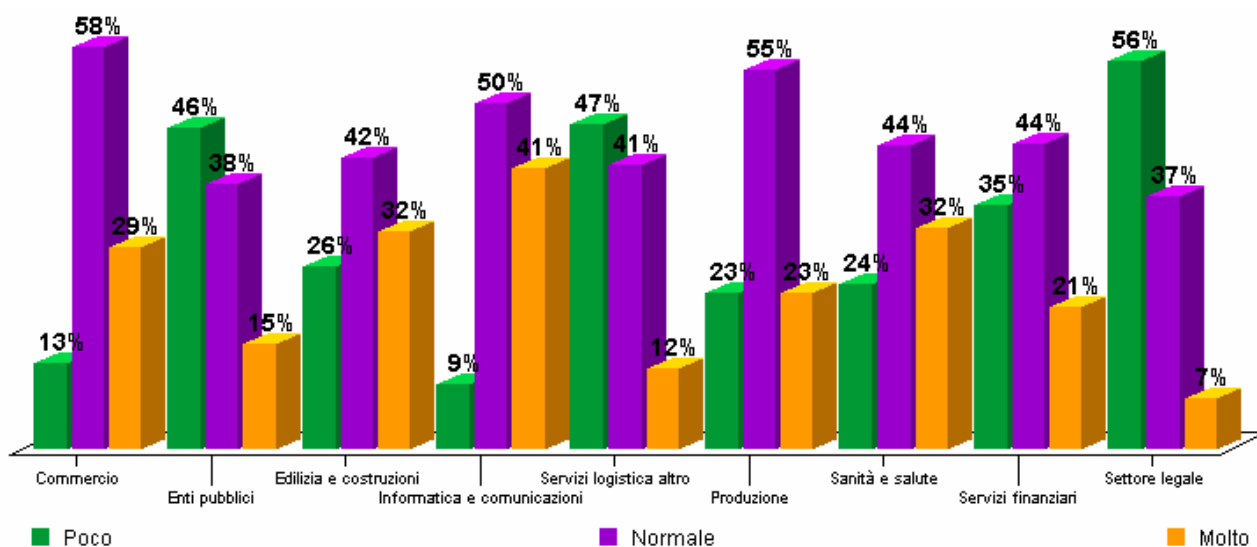


Figura 9: percentuale di utilizzo della rete Internet per attività amministrative e commerciali suddivisa per settore di attività

Domanda 6c. In che misura viene utilizzata la rete Internet per ricercare informazioni

Per quanto riguarda l'utilizzo della rete Internet per ricercare informazioni notiamo che è mediamente presente in tutti i settori con un uso meno accentuato per le aziende dei settori "Edilizia e costruzioni" e "Enti pubblici". Le aziende dei settori "Servizi finanziari", "Servizi logistica altro" e "Commercio" hanno un utilizzo più frequente delle ricerche di informazioni. Le aziende del settore "Informatica e comunicazione" sono naturalmente quelle che ne fanno un uso più elevato soprattutto per il gran numero di informazioni tecniche presenti su Internet.

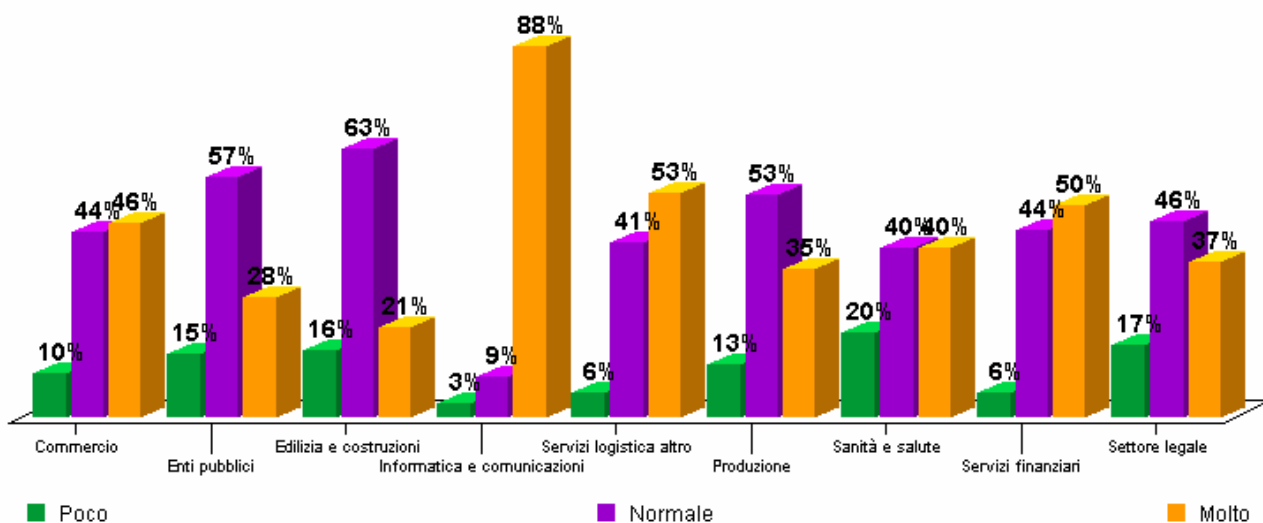


Figura 10: percentuale di utilizzo della rete Internet per ricercare informazioni suddivisa per settore di attività

Se esaminiamo l'utilizzo della rete Internet per ricercare informazioni, dal punto di vista delle dimensioni, si nota che è un'attività presente in modo abbastanza uniforme indipendentemente dal numero di PC. Solo il 20% delle aziende con meno di 5 PC non utilizza questa funzionalità mentre per le altre aziende questa percentuale scende tra il 10% e il 6%.

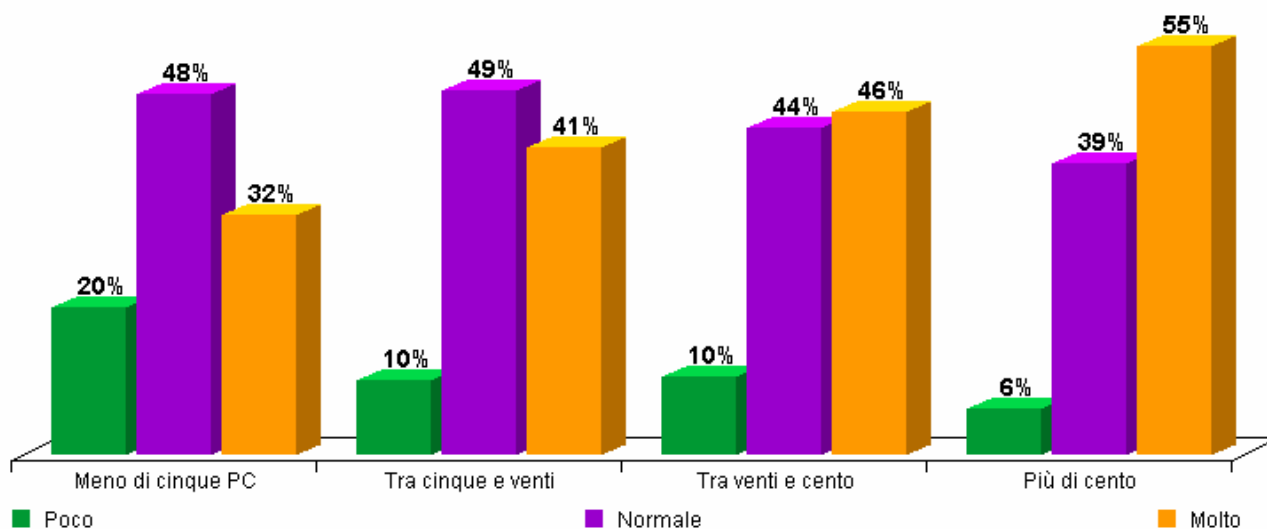


Figura 11: percentuale di utilizzo della rete Internet per ricercare informazioni suddivisa per dimensione

Domanda 6d. In che misura viene utilizzata la rete Internet in azienda per promuovere prodotti e servizi

Per quanto riguarda l'utilizzo della rete Internet per promuovere prodotti e servizi notiamo che essa è poco usata con l'eccezione delle aziende dei settori "Informatica e comunicazione", "Servizi finanziari" e in parte "Produzione".

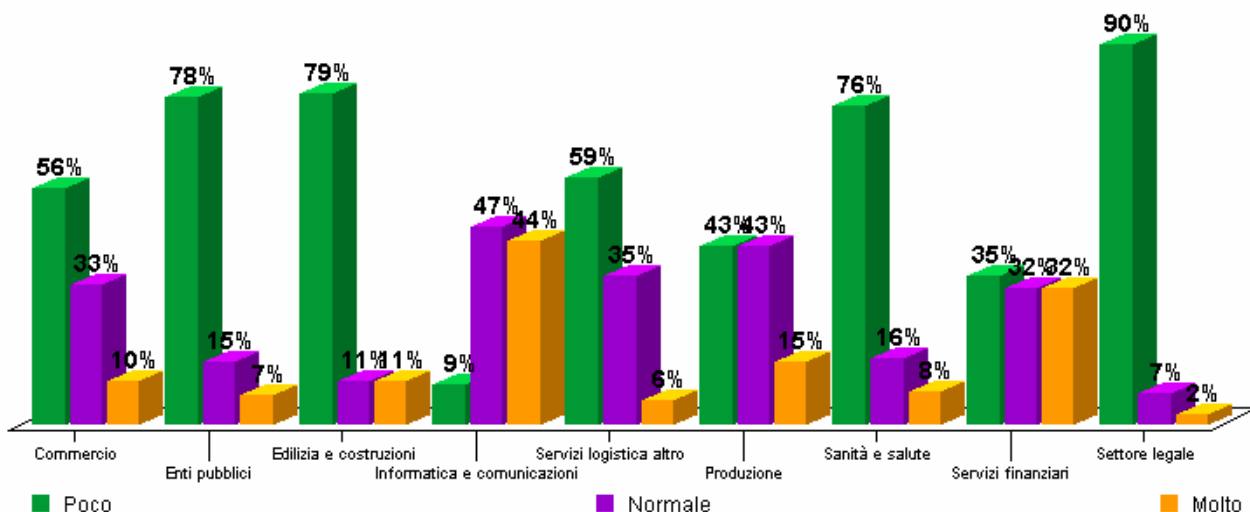


Figura 12 : percentuale di utilizzo della rete Internet per promuovere prodotti e servizi suddivisa per settore di attività

Le risposte danno una conferma di quali sono i settori che hanno probabilmente maggiori interessi e opportunità a utilizzare un sito Internet oppure la posta elettronica, per promuovere i propri prodotti o servizi.

3.4 Caratteristiche dei dati aziendali

Domanda 7. La posta elettronica viene utilizzata per inviare e/o ricevere documenti aziendali importanti o riservati

L'utilizzo della posta elettronica per inviare documenti importanti è pratica comune in oltre il 60% delle aziende dei settori "Informatica e comunicazione", "Servizi logistica altro", "Produzione", "Sanità e salute" e "Settore legale". Il solo settore in cui la posta elettronica è meno utilizzata per inviare documenti importanti è quello degli "Enti pubblici" (62%)

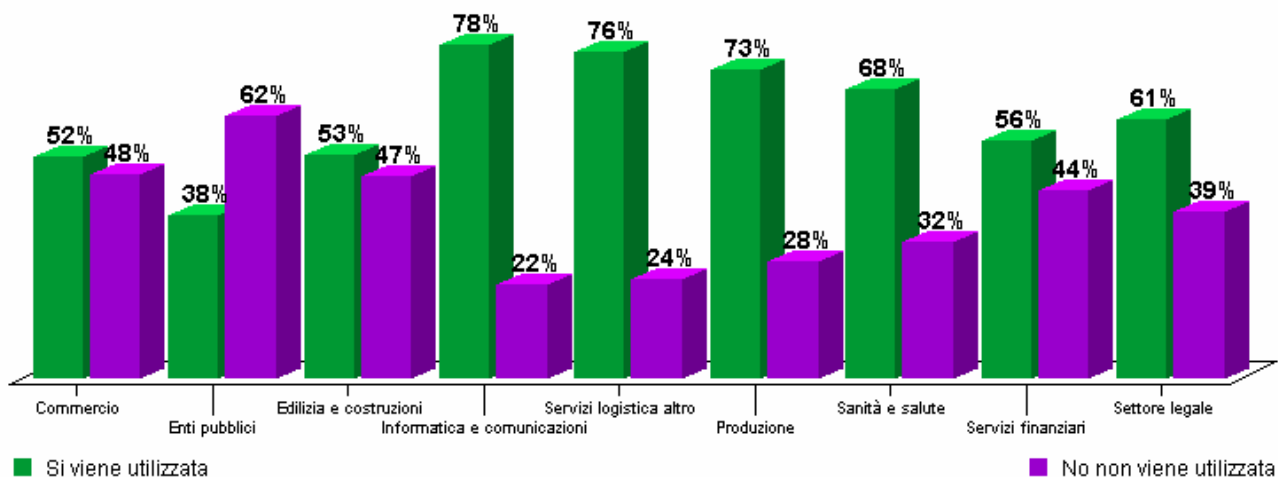


Figura 20 : percentuale del tipo di utilizzo della posta elettronica per inviare e/o ricevere documenti aziendali importanti suddivisa per settore di attività

Domanda 8. Siete al corrente di quali dati devono essere protetti per legge?

In tutti i settori si è al corrente dei tipi di dati protetti per legge con conoscenze che superano l'ottanta per cento dei settori "Servizi finanziari" (91%), "Settore legale" (90%), "Enti pubblici" (83%).

Nei settori "Commercio", "Edilizia e costruzioni" e "Produzione" è minore la consapevolezza della necessità di proteggere i dati delle persone.

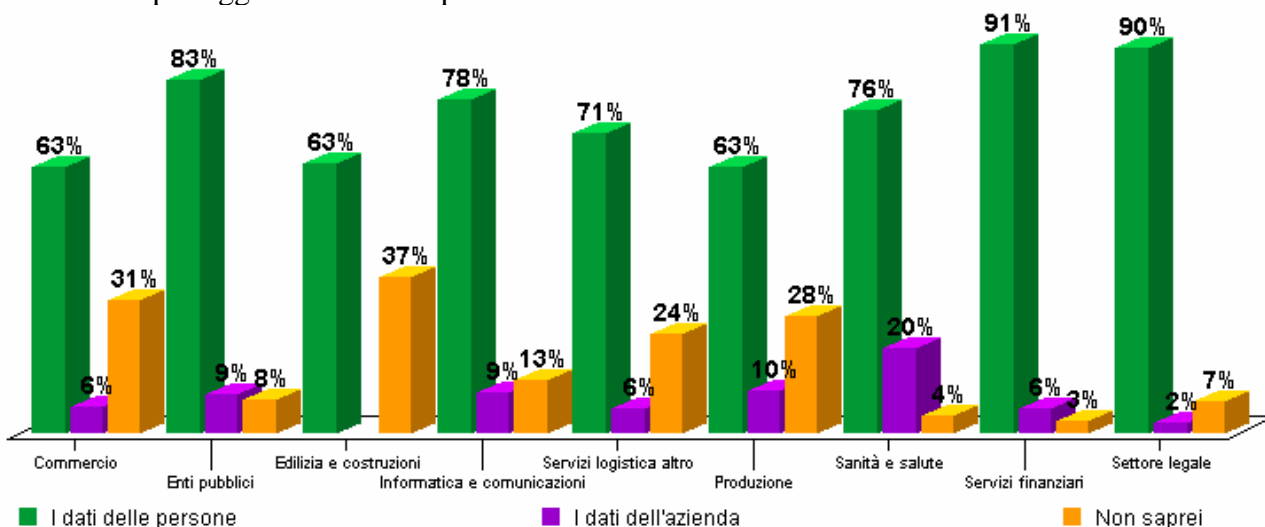


Figura 13 : percentuale di conoscenza dei dati protetti per legge suddivisa per settore di attività

Domanda 9. Ci sono informazioni critiche sui PC o sui server aziendali?

Complessivamente oltre il 90% delle informazioni presenti sui PC e sui server aziendali sono considerate critiche. Le informazioni tutelate dalla legge sulla protezione dei dati sono considerate

critiche soprattutto nei settori “Enti pubblici” (48%), “Sanità e salute” (36%), “Settore legale” (35%) e “Servizi finanziari” (34%).

Le informazioni operative dell’azienda sono considerate critiche soprattutto nei settore “Commercio” (40%), “Informatica e comunicazione” (40%), “Edilizia e costruzione” (39%) e “Produzione” (38%).

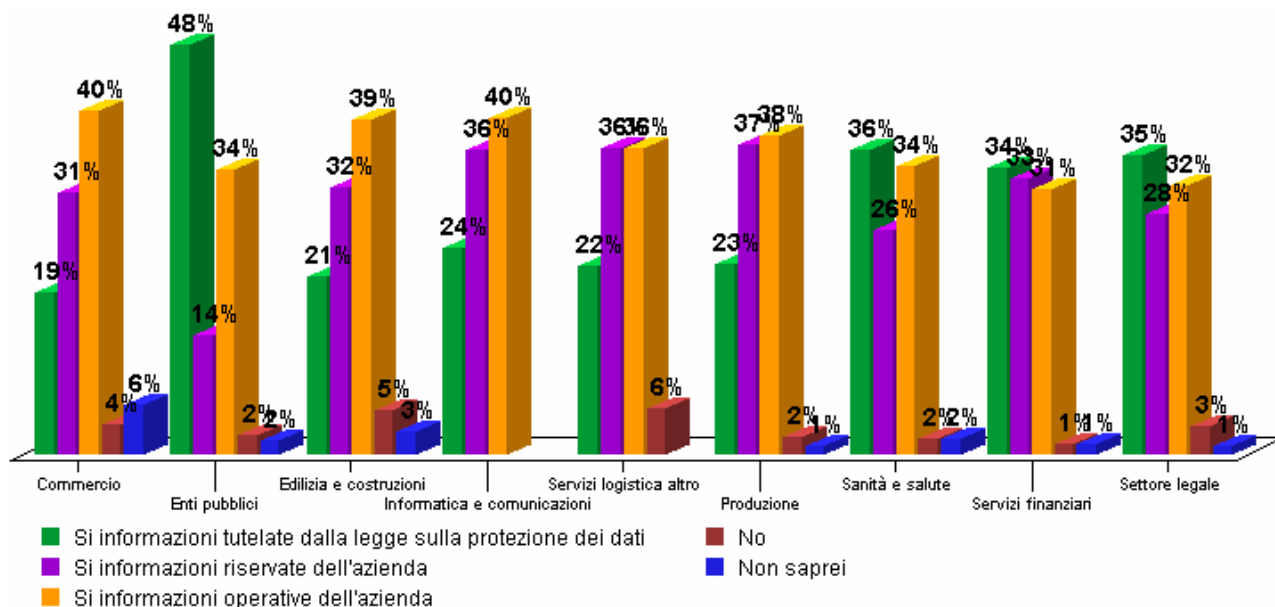


Figura 14 : percentuale di informazioni critiche sui PC e sui server aziendali suddivisa per settore di attività

Complessivamente, in ordine di importanza vengono considerate critiche le informazioni operative dell’azienda dal 72% degli intervistati, quelle tutelate dalla legge sulla protezione dei dati dal 65% e le informazioni riservate dell’azienda dal 57%.

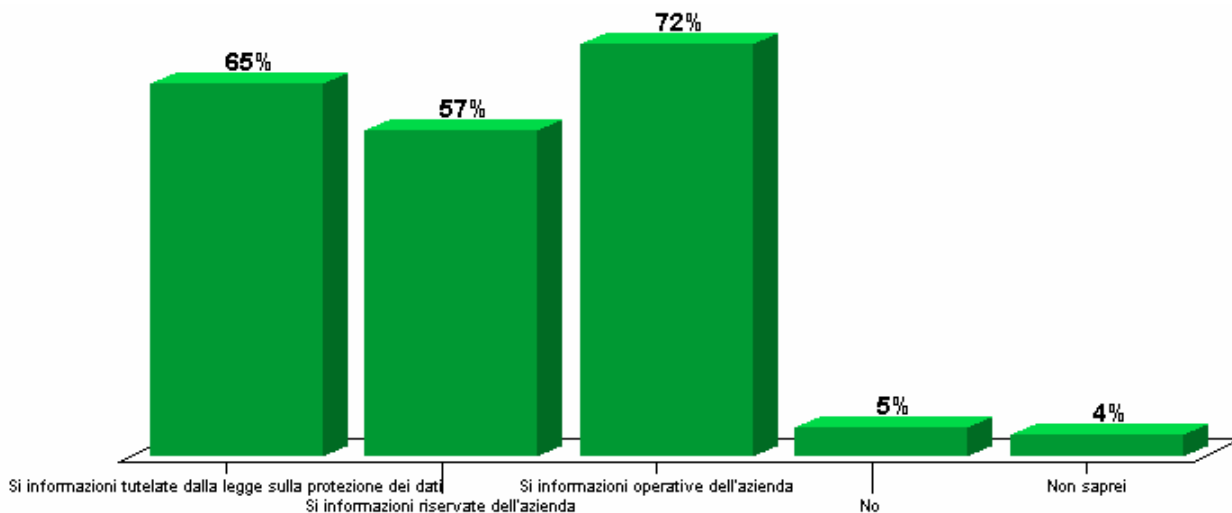


Figura 15 : percentuale di informazioni critiche sui PC e sui server aziendali (Il totale della percentuale supera il 100% perché la domanda permetteva scelte multiple)

Domanda 10. Quale danno potrebbe derivare da una distruzione o da una perdita di queste informazioni critiche?

Una distruzione o una perdita delle informazioni critiche viene considerato un danno grave nei settori “Servizi finanziari” (76%), “Enti pubblici” (61%), “Sanità e salute” (60%), “Servizi logistica altro” (59%).

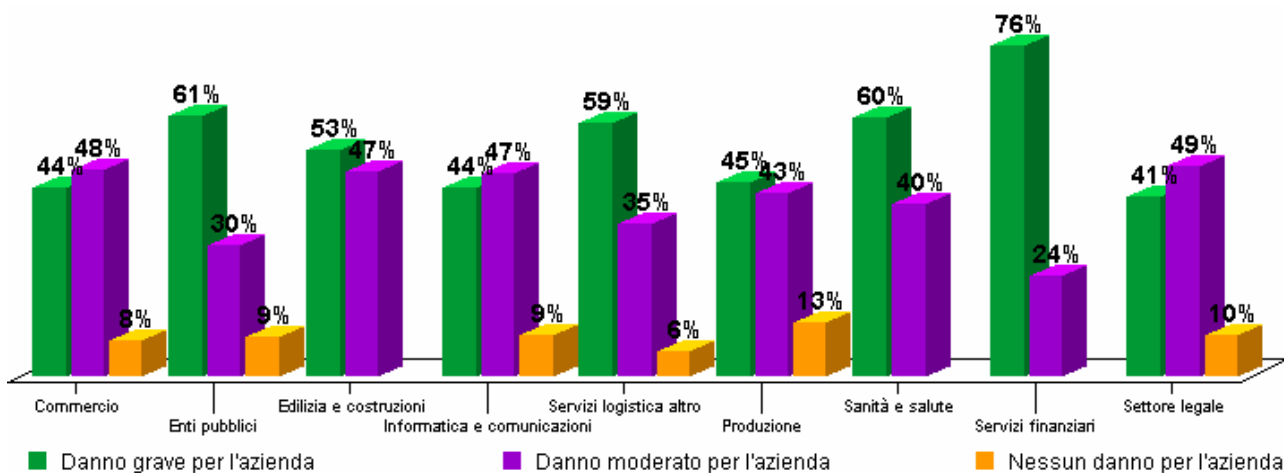


Figura 16 : percentuale del tipo di danno derivato dalla distruzione delle informazioni critiche sui PC e sui server aziendali suddivisa per settore di attività

Il danno grave che può derivare da una distruzione o da una perdita di queste informazioni critiche viene percepito maggiormente nelle aziende con più PC che in quelle con pochi PC.

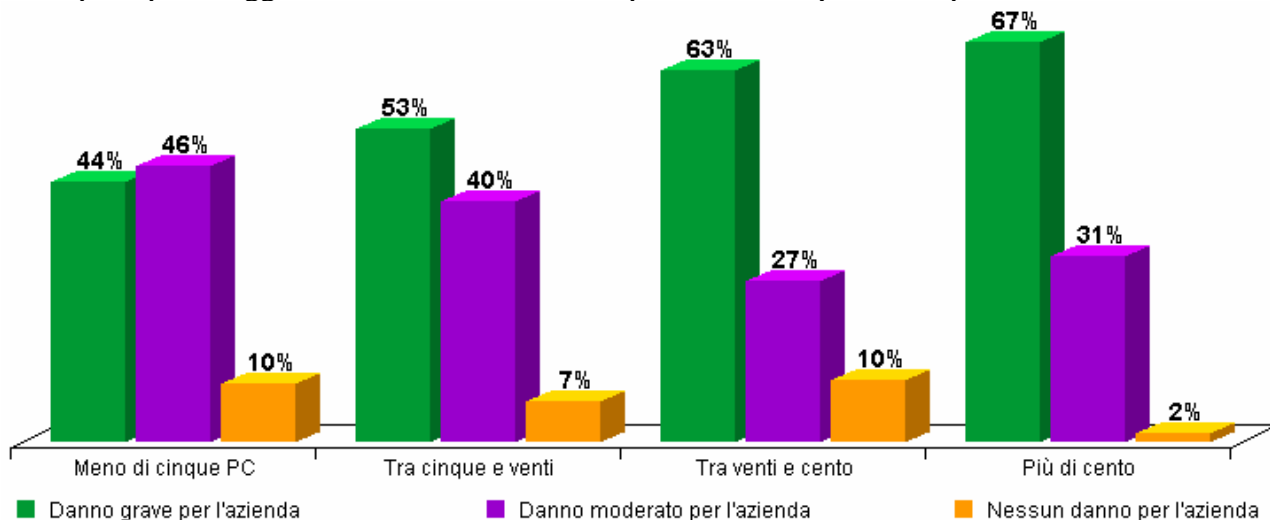


Figura 17 : percentuale del tipo di danno derivato dalla distruzione delle informazioni critiche sui PC e sui server aziendali suddivisa per dimensione

Domanda 11. Quale danno potrebbe derivare da un furto o da una diffusione pubblica di queste informazioni critiche?

Un furto o una diffusione pubblica delle informazioni critiche viene considerato un danno grave nei settori “Servizi finanziari” (79%), “Settore legale” (54%), “Enti pubblici” (54%), “Sanità e salute” (52%). In tutti i settori, ad eccezione di “Servizi finanziari” e “Settore legale” il furto o la diffusione pubblica delle informazioni critiche viene considerata meno grave della loro perdita o distruzione.

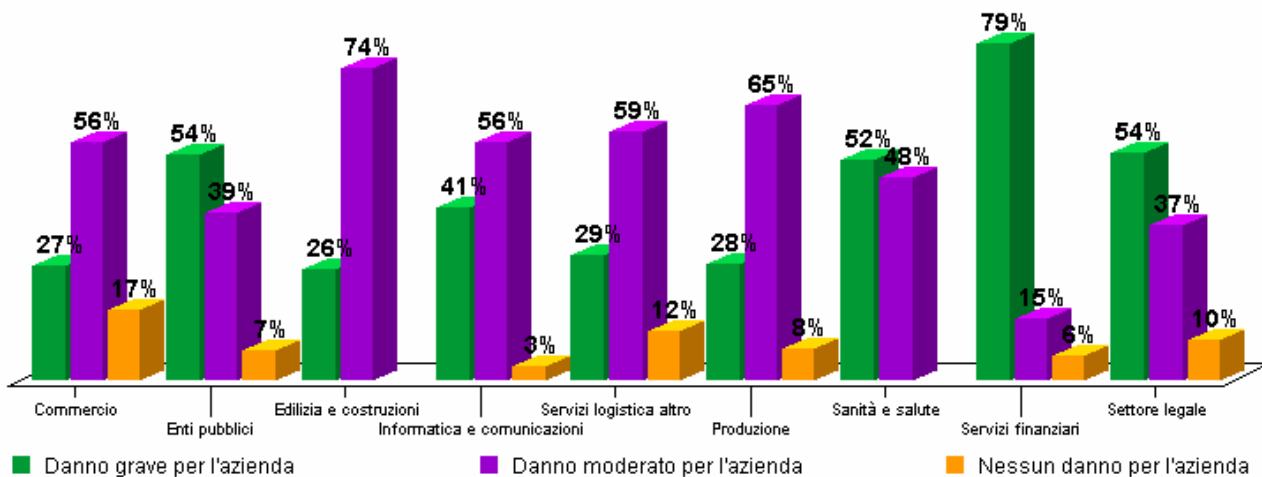


Figura 18 : percentuale del tipo di danno derivato da furto o diffusione delle informazioni critiche sui PC e sui server aziendali suddivisa per settore di attività

Il danno grave che può derivare da un furto o da una diffusione pubblica di queste informazioni critiche viene percepito maggiormente nelle aziende con più PC che in quelle con pochi PC. Nelle aziende con meno di 100 PC il furto o la diffusione pubblica delle informazioni critiche viene considerata meno grave della loro perdita o distruzione.

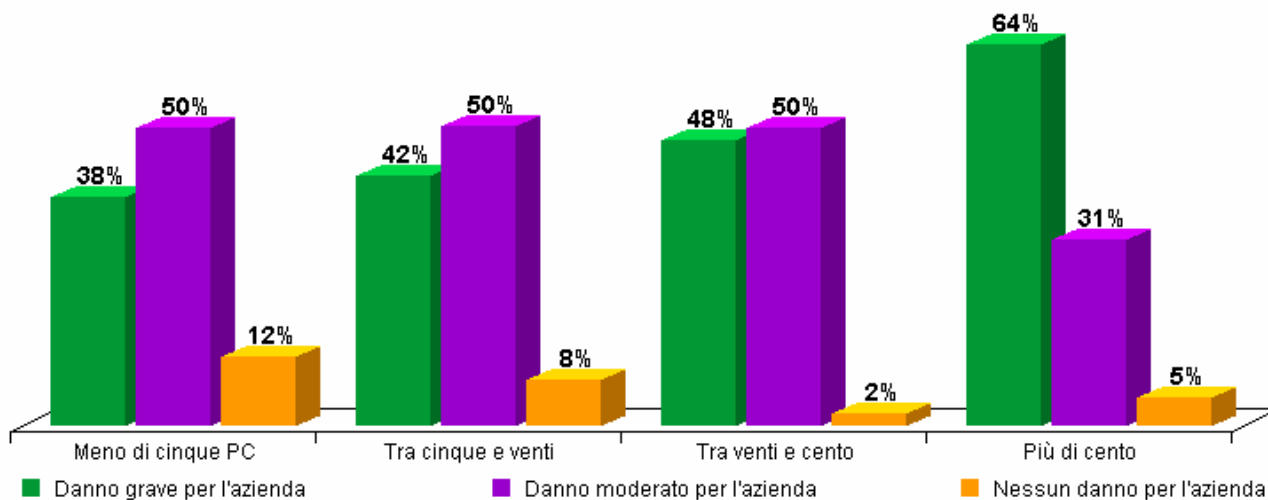


Figura 19 : percentuale del tipo di danno derivato da furto o diffusione delle informazioni critiche sui PC e sui server aziendali suddivisa per dimensione

3.5 Aspetti organizzativi

Domanda 12. Quali sono le competenze dei dipendenti nell'uso dei PC e di Internet?

Le competenze dei dipendenti nell'uso dei PC e di Internet a dipendenza del settore di attività del campione sono prevalentemente molto buone per il settore "Informatica e comunicazione" mentre in tutti gli altri settori del campione sono equamente distribuite tra normali e buone. Si discosta il settore "Commercio" dove le competenze sono prevalentemente normali.

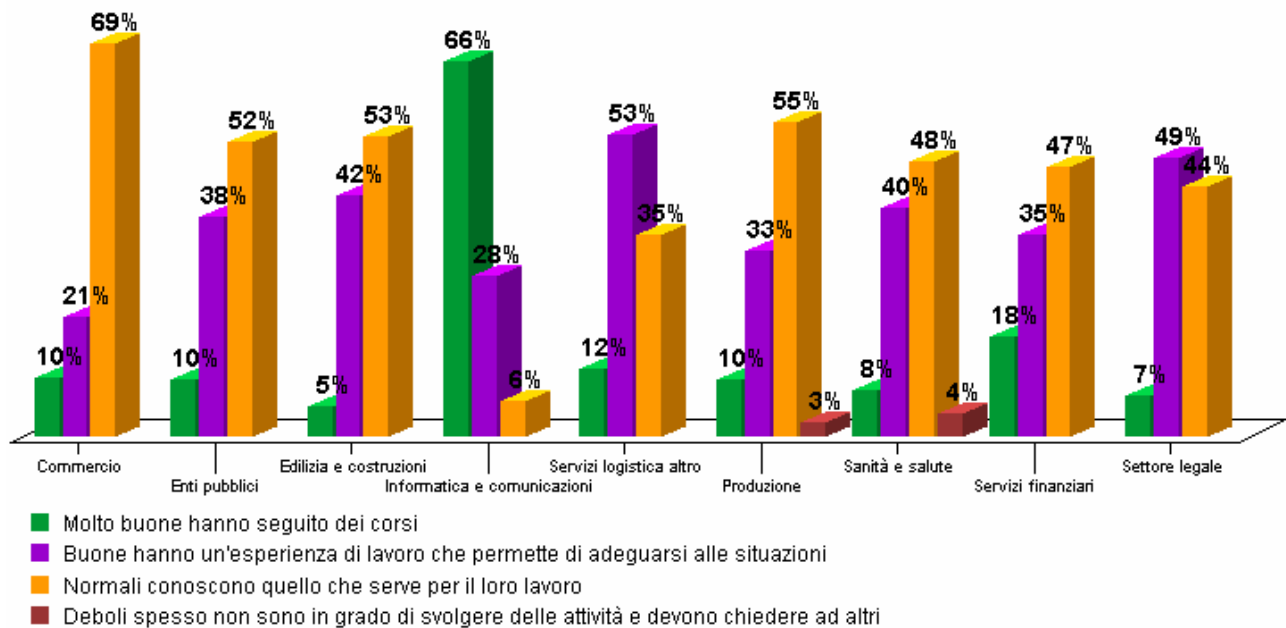


Figura 22 : percentuale sulle competenze dei dipendenti sull'uso dei PC e di Internet suddivisa per settore di attività

Esaminando le competenze dei dipendenti nell'uso dei PC e di Internet con riferimento alla dimensione dell'azienda si nota che le competenze normali o buone sono distribuite in modo uniforme nelle aziende con meno di 100 PC. Nel campione di aziende di maggiori dimensioni (oltre 100 PC) si nota un aumento dei dipendenti con competenze normali e con competenze molto buone.

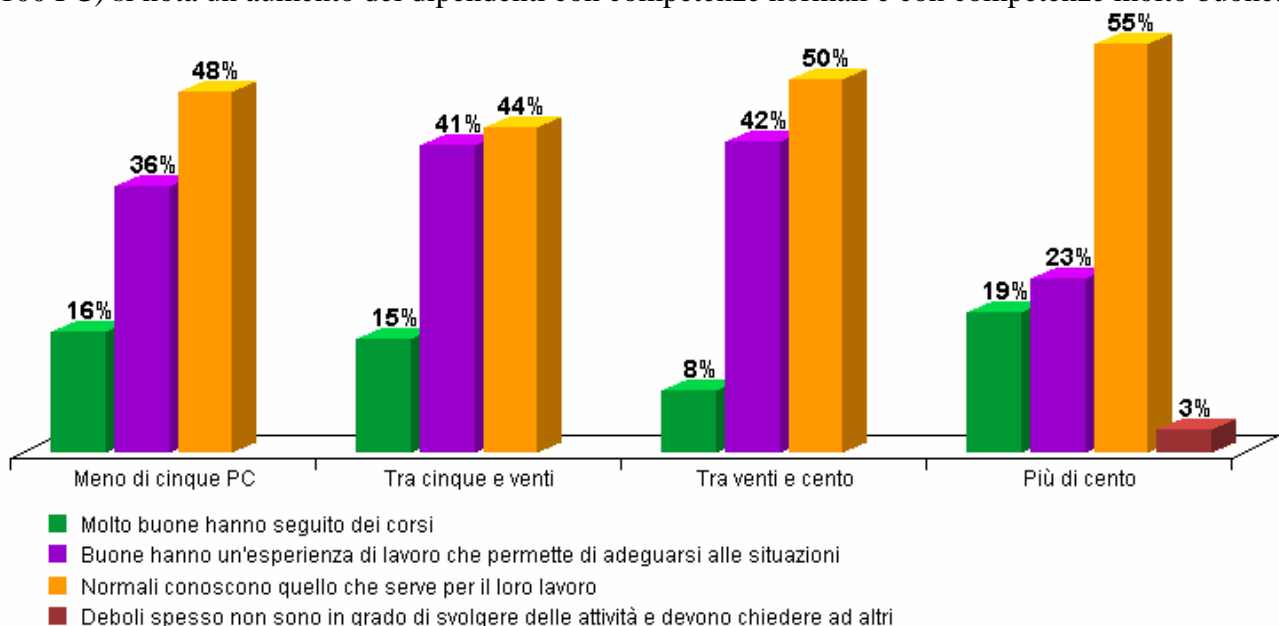


Figura 23 : percentuale sulle competenze dei dipendenti sull'uso dei PC e di Internet suddivisa per dimensione

Domanda 13. Avete delle esigenze di controllo dei dipendenti aziendali?

Per quanto riguarda l'esigenza di controllo dei dipendenti aziendali notiamo che è presente principalmente nel campione delle aziende del settore "Servizi finanziari" è in circa la metà delle aziende dei settori "Produzione" e "Sanità e salute".

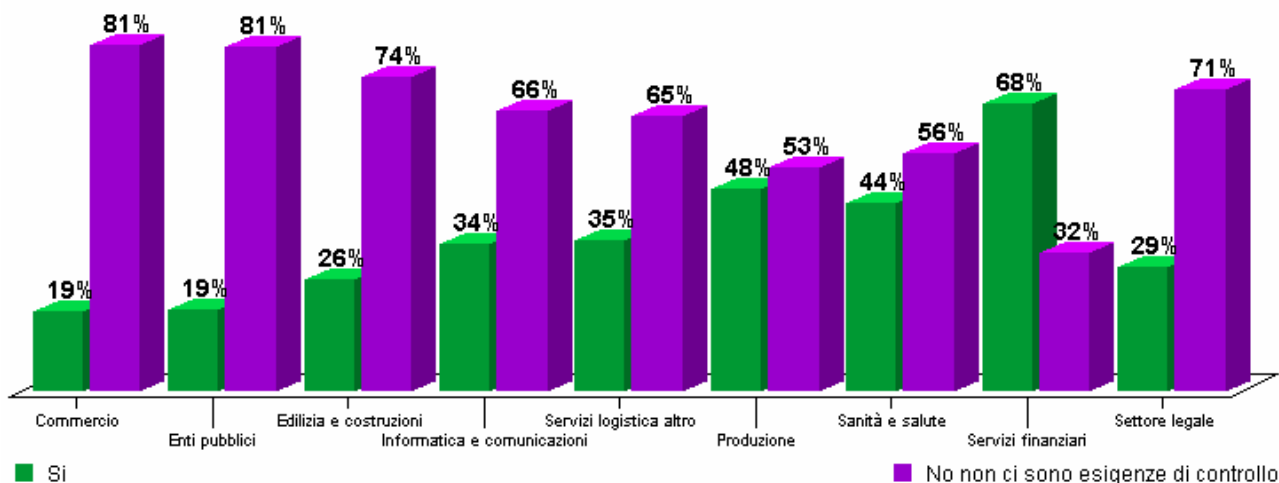


Figura 23 : percentuale sulle esigenze di controllo dei dipendenti suddivisa per settore di attività

Le esigenze di controllo dei dipendenti aziendali aumentano in proporzione all'aumento delle dimensioni delle aziende

Avete delle esigenze di controllo dei dipendenti	Meno di cinque PC %	Tra cinque e venti %	Tra venti e cento %	Più di cento %
Si	8.93	23.66	54.17	75.00
No	91.07	76.34	45.83	25.00

Figura 24 : percentuale sulle esigenze di controllo dei dipendenti suddivisa per dimensioni

Domanda 14. Quali di queste attività ritenete che siano gravi nell'utilizzo di Internet da parte dei dipendenti?

Con riferimento alla dimensione dell'azienda le attività ritenute più gravi nell'utilizzo di Internet da parte dei dipendenti sono il consultare siti di dubbia moralità e gioco d'azzardo e *chattare* con persone all'esterno dell'azienda: I medesimi risultati sono confermati anche analizzando le risposte delle aziende suddivise per settore di attività come si vede nella figura 25.

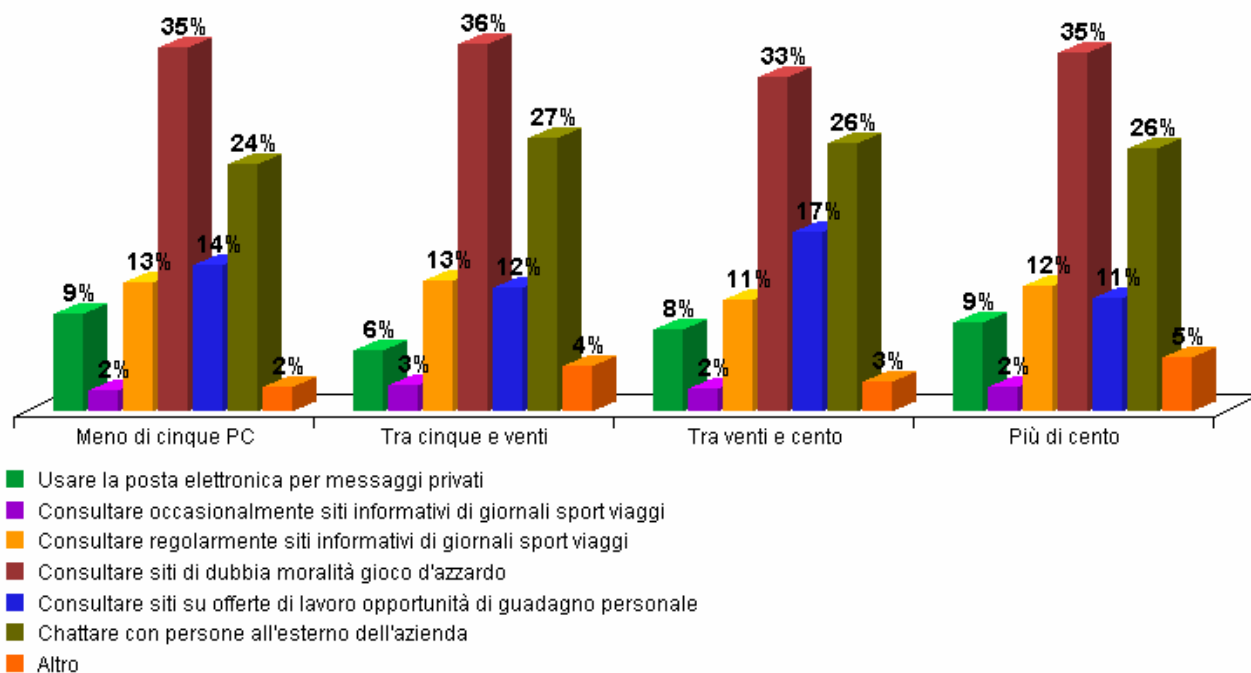


Figura 26 : percentuale delle attività ritenute gravi nell'utilizzo di Internet da parte dei dipendenti suddivisa per dimensioni

Analogamente a quanto risulta dall'analisi per dimensione dell'azienda, anche l'analisi per settore di attività mostra che le attività ritenute più gravi nell'utilizzo di Internet da parte dei dipendenti sono il consultare siti di dubbia moralità e gioco d'azzardo e *chattare* con persone fuori dell'azienda.

Attività ritenute gravi nell'utilizzo di Internet da parte dei dipendenti	Commercio %	Enti pubblici %	Edilizia e costruzioni %	Informatica %	Servizi logistica altro %	Produzione %	Sanità e salute %	Servizi finanziari %	Settore legale %
Usare la posta elettronica per messaggi privati	8.55	5.31	10.71	6.76	6.67	9.40	10.67	10.20	7.37
Consultare occasionalmente siti informativi di giornali sport viaggi	4.27	1.22	1.79	1.35	4.44	3.42	4.00	2.04	0.00
Consultare regolarmente siti informativi di giornali sport viaggi	12.82	11.02	12.50	10.81	11.11	13.68	10.67	14.29	13.68
Consultare siti di dubbia moralità gioco d'azzardo	35.04	37.96	28.57	39.19	33.33	31.62	32.00	31.63	38.95
Consultare siti su offerte di lavoro opportunità di guadagno personale	11.11	14.29	19.64	13.51	15.56	13.68	14.67	12.24	8.42
Chattare con persone all'esterno dell'azienda	25.64	27.76	23.21	20.27	26.67	23.93	26.67	24.49	26.32
Altro	2.56	2.45	3.57	8.11	2.22	4.27	1.33	5.10	5.26

Figura 25 : percentuale delle attività ritenute gravi nell'utilizzo di Internet da parte dei dipendenti suddivisa per settore di attività

Domanda 15. Avete dei regolamenti che disciplinano l'uso dei PC e di Internet per i dipendenti?

I regolamenti che disciplinano l'uso dei PC e di Internet sono presenti nella maggior parte delle aziende del settore "Servizi finanziari" (76%). Sono assenti nella maggior parte delle aziende dei settori "Enti pubblici" (78%), "Settore legale" (68%) e "Sanità e salute" (64%)

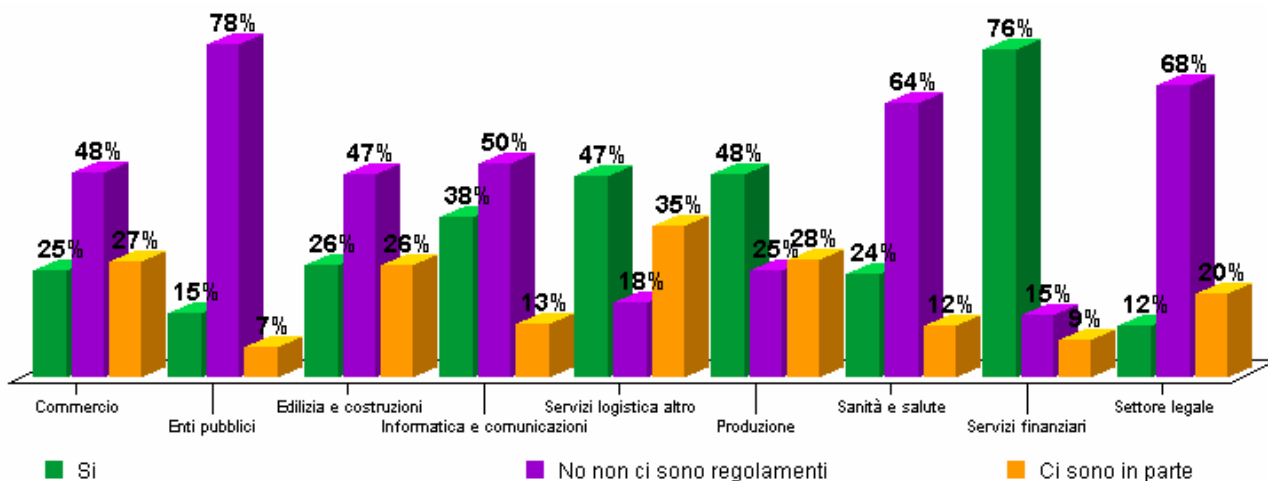


Figura 27 : percentuale di aziende con regolamenti che disciplinano l'uso dei PC e di Internet da parte dei dipendenti suddivisa per settore di attività

Se si analizza la presenza di regolamenti che disciplinano l'uso dei PC e di Internet a dipendenza della dimensione dell'azienda si nota che sono soprattutto presenti nelle aziende di maggiori dimensioni

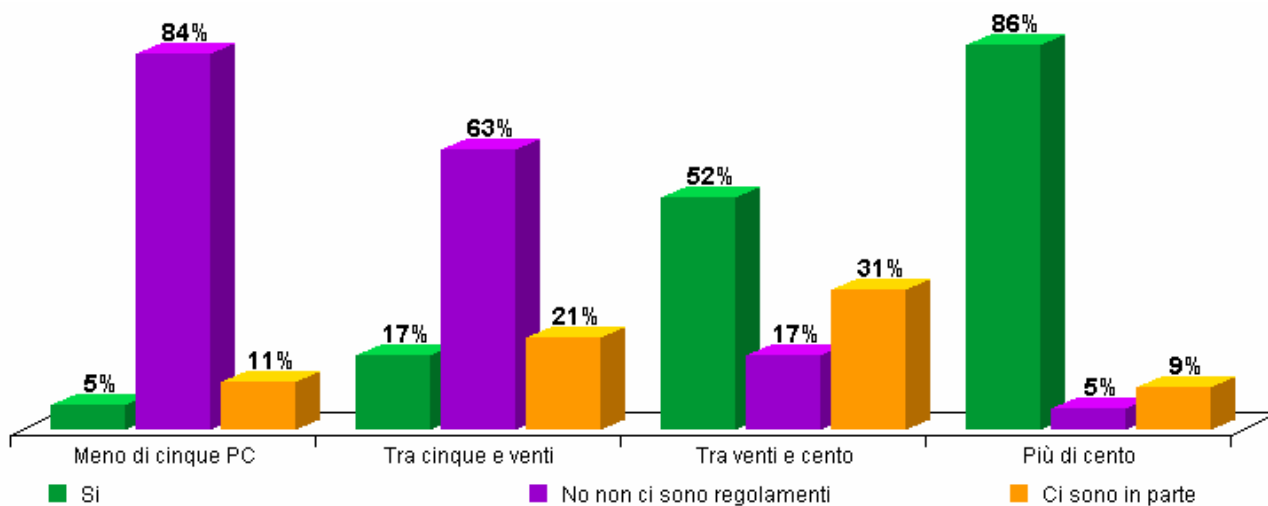


Figura 28 : percentuale di aziende con regolamenti che disciplinano l'uso dei PC e di Internet da parte dei dipendenti suddivisa per dimensioni

Domanda 19. Esiste un responsabile della sicurezza informatica in azienda?

La presenza di un responsabile della sicurezza informatica è elevata nei settori "Informatica e comunicazione" (97%) e "Servizi finanziari" (88%) ed è presente in circa due terzi delle aziende dei settori "Produzione" (73%), "Edilizia e costruzioni" (68%), "Servizi logistica altro" (65%) e "Sanità e salute" (64%)

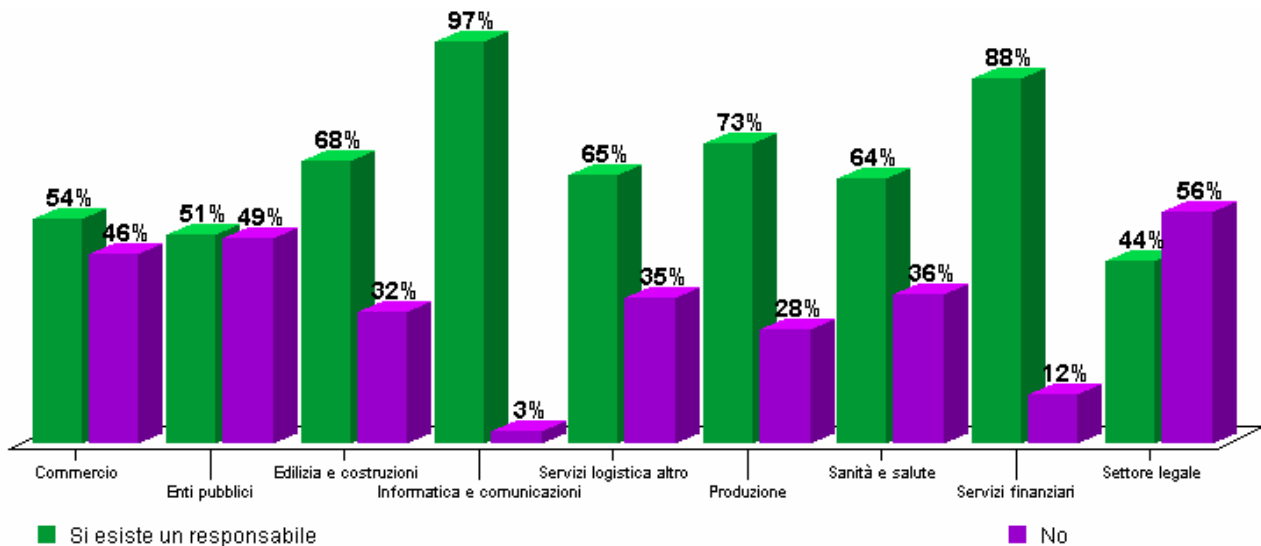


Figura 20 : percentuale sulla presenza di un responsabile della sicurezza informatica in azienda suddivisa per settore di attività

Se si analizza la presenza di un responsabile della sicurezza informatica a dipendenza della dimensione dell'azienda si nota che questa figura esiste prevalentemente nelle aziende di maggiori dimensioni

<i>Esiste un responsabile della sicurezza Informatica in azienda</i>	Meno di cinque PC %	Tra cinque e venti %	Tra venti e cento %	Più di cento PC %
Si	33.93	66.41	89.58	87.5
No	66.07	33.59	10.42	12.5

Figura 21 : percentuale sulla presenza di un responsabile della sicurezza informatica in azienda suddivisa per dimensione

3.6 Aspetti tecnici

Domanda 16. Quali di queste misure di sicurezza avete previsto per la vostra infrastruttura informatica?

Le risposte permettono di valutare quali sono le tecnologie maggiormente utilizzate per la protezione dei dati aziendali.

Dalle risposte risulta che nelle aziende le misure di sicurezza più utilizzate sono l'antivirus su tutti i PC (88%), seguite dal salvataggio periodico dei dati (81%) e dall'uso della password di accesso ai PC (77%).

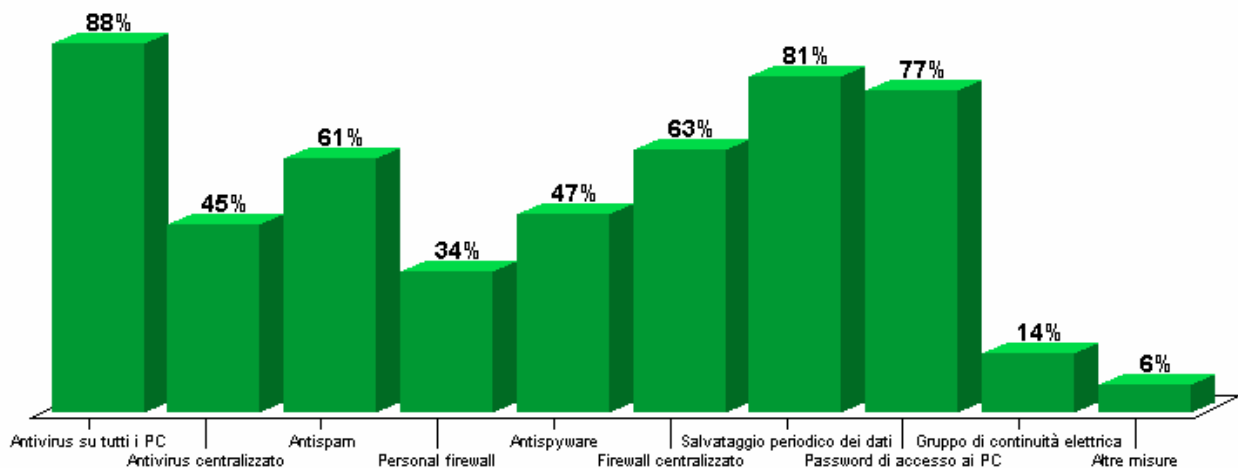


Figura 29 : percentuale delle misure tecniche previste per l'infrastruttura informatica aziendale (Il totale della percentuale supera il 100% perché la domanda permetteva scelte multiple)

Domanda 17. Vengono fatti gli aggiornamenti degli antivirus e del software di sistema?

L'aggiornamento degli antivirus e del software di sistema dà un'indicazione dell'attenzione continua che viene data agli aspetti tecnici della sicurezza informatica. Tutte le aziende intervistate nei settori "Informatica e comunicazioni" e "Servizi finanziari" fanno regolarmente gli aggiornamenti. Queste pratiche di aggiornamento sono fatte anche nella maggior parte delle aziende di altri settori.

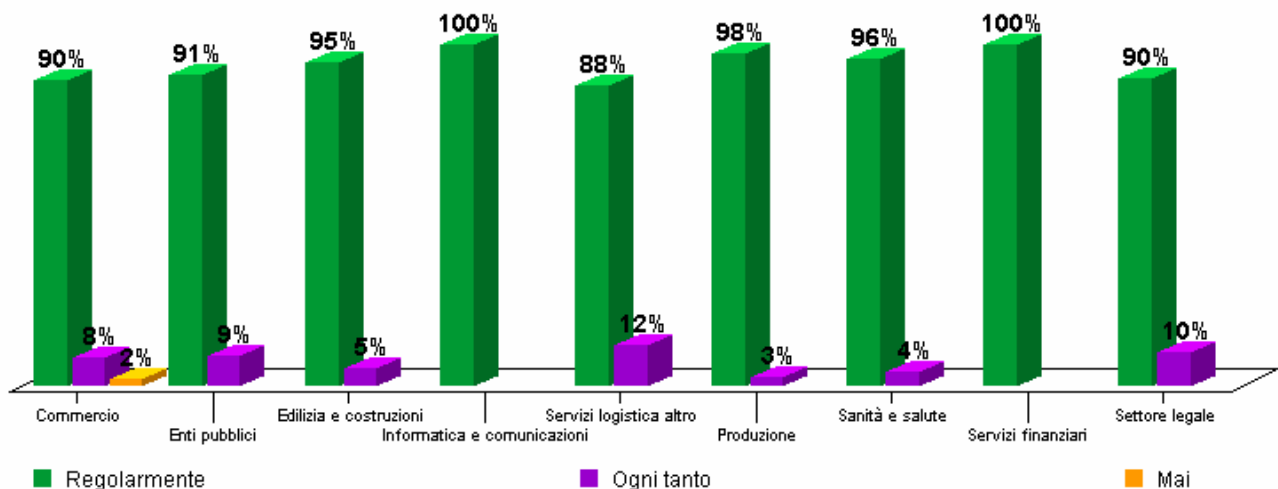


Figura 30 : percentuale degli aggiornamenti degli antivirus e del software di sistema suddivisa per settore di attività

Domanda 18. Ci sono dei problemi particolari di sicurezza nell'uso dei PC e di Internet nella vostra azienda?

Nelle aziende con meno di cinque PC i problemi di sicurezza sono percepiti in meno del 10 per cento delle aziende intervistate. La consapevolezza dei problemi di sicurezza sale con l'aumento della dimensione dell'azienda e nelle aziende tra 20 e 100 PC interessa quasi un quarto delle aziende intervistate. Tra i problemi riscontrati sono segnalati i *virus*, lo *spam*, le intrusioni e gli accessi non autorizzati.

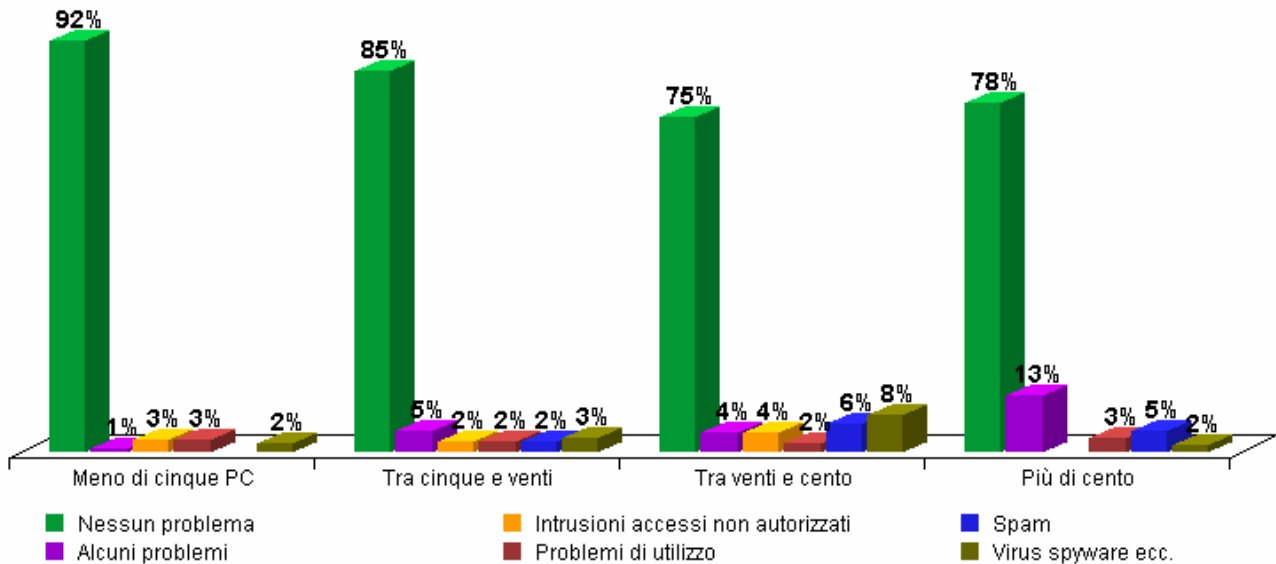


Figura 31 : percentuale di problemi particolari di sicurezza nell'uso dei PC e di Internet da parte dei dipendenti suddivisa per dimensioni

Ulteriori analisi dei dati

Le analisi dei dati presentati fino qui sono state eseguite confrontando principalmente le risposte a ciascuna domanda con i settori di attività oppure con la dimensione dell'azienda.

Per chi fosse interessato a ulteriori raffronti è possibile paragonare le diverse risposte tra loro utilizzando uno strumento dinamico di analisi dei dati, basato su Web, come indicato nel capitolo 5.

4 Considerazioni finali

Settore di attività

Fra i settori interessati dall'inchiesta, quello degli "Enti pubblici" ha dato il numero più elevato di risposte, provenienti soprattutto dai comuni. Questo potrebbe essere ricondotto al fatto che l'inchiesta è stata suggerita loro dalla Sezione degli enti locali del Canton Ticino.

Dall'inchiesta si è notato che in questo settore esiste una particolare attenzione al tema della sicurezza informatica. Le aziende del settore "Informatica e comunicazione" hanno risposto in modo significativo in proporzione al loro numero in Ticino. Anche i settori "Commercio", "Settore legale", "Produzione" e "Servizi finanziari" hanno dato una buona risposta.

Dimensioni dell'azienda

Per la criticità dei loro dati, settori quali "Sanità e salute" o "Servizi finanziari" hanno esigenze di sicurezza che sono indipendenti dalla dimensione dell'azienda, mentre nel caso dei settori di attività "Produzione" e "Commercio" si nota una differente sensibilità ai problemi della sicurezza che aumenta con la dimensione dell'azienda.

Uso di Internet

Dall'inchiesta è emerso un uso diffuso di Internet (posta elettronica, attività amministrative e commerciali, ricerca informazioni, promozione di prodotti e servizi) che indica come le aziende si confrontino con i rischi che sono caratteristici della rete Internet. L'inchiesta mostra un uso abbastanza diffuso di tecniche di protezione specifiche quali antivirus, *firewall* centralizzati, *personal firewall*, *antispam* e *antispyware*. La maggiore sensibilità del personale nei confronti dei rischi di Internet è presente soprattutto nelle aziende che lo utilizzano maggiormente.

Caratteristiche dei dati aziendali

Il fatto che la posta elettronica è utilizzata in molti settori per inviare documenti importanti denuncia una scarsa conoscenza dei rischi che questo mezzo comporta, soprattutto per l'assenza di riservatezza nella trasmissione. I settori che ritengono di poter avere danno maggiore da un furto di informazioni sono quelli che generalmente fanno un uso minore della posta elettronica per inviare documenti importanti ("Enti pubblici" e "Servizi finanziari").

La consapevolezza di quali sono i dati che devono essere protetti per legge è presente nei settori "Enti pubblici", "Sanità e salute" e "Settore legale" che sono più a contatto con i temi delle leggi federali e cantonali sulla protezione dei dati, oppure nel settore "Servizi finanziari" a contatto con la Legge federale sulle banche e le casse di risparmio. Negli altri settori si tende a dare maggiore importanza alle informazioni operative o riservate dell'azienda.

Aspetti organizzativi

Competenze molte buone nell'uso dei PC grazie a corsi di formazione, si riscontrano solo nel settore "Informatica e comunicazione". Negli altri settori prevalgono competenze buone o normali, probabilmente non sufficienti per reagire in modo corretto e tempestivo di fronte a situazioni di rischio quali attacchi di *social engineering*, sia perché i dipendenti non sono in grado di identificare il potenziale pericolo, sia perché non esistono le conoscenze su come bisogna comportarsi in situazioni critiche. Questo vale soprattutto per le piccole aziende dove non esistono regolamenti scritti e dove l'informazione è scarsa a livello tecnico.

Il settore di attività con la maggiore percentuale di aziende dotate di regolamenti che disciplinano l'uso dei PC e di Internet è quello finanziario (75%). Solleva invece qualche interrogativo il fatto che i settori più vicini alle problematiche di tipo legale e amministrativo non dispongano di regolamenti. Si sono detti sprovvisti di regolamenti il 78% degli "Enti pubblici", il 68% del "Settore legale" e il 64% del settore "Sanità e salute".

La presenza di un responsabile della sicurezza informatica si trova prevalentemente nelle aziende di medie dimensioni (87% delle aziende con più 100 PC). Nella quasi totalità delle aziende del settore "Informatica e comunicazione" (97%) è presente un responsabile della sicurezza, mentre negli altri settori la presenza di questa figura è collegata direttamente alle dimensioni aziendali.

Aspetti comportamentali

Una forte esigenza di controllo dei dipendenti nell'uso di Internet e della posta elettronica è presente solo nel settore "Servizi finanziari". Se esaminiamo questa esigenza in relazione alle dimensioni aziendali, possiamo notare che essa prevale nelle aziende con oltre 20 PC.

Considerando le attività ritenute gravi nell'utilizzo di Internet si nota come in tutti i settori sia considerato di maggiore gravità la consultazione di siti di dubbi moralità o gioco d'azzardo con percentuali che variano dal 28.57% per il settore "Edilizia e costruzioni" al 39.19% del settore "Informatica e comunicazione". Il tasso più elevato può derivare dal fatto che nel settore "Informatica e comunicazione" vi è una migliore conoscenza di quanto presente su Internet.

Al secondo posto per gravità troviamo *chattare* con persone all'esterno dell'azienda. Le percentuali hanno il loro massimo nel settore "Enti pubblici" (27.76%) e scendono fino al 20.27% nel settore "Informatica e comunicazione" dove uso delle tecnologie di *instant messaging* viene considerato meno grave poiché utilizzate probabilmente anche per le normali attività lavorative.

Consultare regolarmente siti informativi di giornali, sport, viaggi, ecc. è considerato in generale grave per una percentuale che va dal 10.81% al 14.29%, mentre la consultazione occasionale di siti con offerte di lavoro, opportunità di guadagno, ecc. è considerata grave per una percentuale che si colloca intorno al 14% in tutti i settori ad eccezione di due casi estremi per "Edilizia e costruzioni" (19.64%) e "Settore legale" (8.42%). La consultazione occasionale di siti informativi di giornali, sport, viaggi, ecc. vengono considerate attività accettabili da oltre il 95% delle aziende in tutti i settori di attività. L'uso della posta elettronica per messaggi privati è tollerata nel 90% delle aziende. Questo può aprire interrogativi di sicurezza soprattutto nel caso in cui i dipendenti non sono informati sui possibili rischi che un uso superficiale della posta elettronica può comportare. Sempre più codice malefico viene oggi diffuso attraverso *spam* o catene di Sant'Antonio, con testi, messaggi, filmati o immagini che tendono a sollecitare la naturale curiosità delle persone per ingannarli e infettare i loro PC, catturandoli in una *botnet* e mettendoli sotto il controllo della criminalità organizzata. A questo si aggiunge l'invito a diffondere questi messaggi presso amici e conoscenti che, fidandosi di chi ha inviato il messaggio, diventano anche loro vittime dell'attacco.

Aspetti tecnici

L'insieme delle misure tecniche adottate fornisce un quadro abbastanza esauriente di quali sono i principali rischi percepiti. Nel 88% delle aziende sono installati antivirus su tutti i PC, mentre gli antivirus centralizzati sono presenti nel 45% delle aziende, principalmente quelle con oltre 20 PC. Il salvataggio periodico dei dati viene fatto nel 81% delle aziende. Va da sé che il 19% di aziende o non ha necessità di fare il salvataggio periodico dei dati o non è cosciente dell'importanza di questa pratica. L'uso della password di accesso ai PC è utilizzato nel 77% delle aziende. Questo significa che esiste un 23% di aziende che utilizza altri mezzi di autenticazione o che non si rende conto di quanto sia importante l'autenticazione per proteggere l'accesso ai PC e ai dati.

L'aggiornamento di antivirus e sistema operativo mostra l'attenzione che l'azienda ha continuamente nei confronti dei suoi sistemi informatici. Nei settori "Informatica e comunicazione" e "Servizi finanziari" la totalità delle aziende fa gli aggiornamenti in modo regolare. Negli altri settori la percentuale di aziende che fa regolarmente gli aggiornamenti è intorno al 90%.

Alla domanda se esistono problemi particolari nell'uso dei PC e di Internet, la maggior parte delle aziende con pochi PC dichiara di non avere alcun problema (92% delle aziende con meno di 5 PC) mentre nelle aziende con più di 20 PC il tasso scende intorno al 75%. Questo può significare o che le aziende più grosse sono più spesso oggetto di attacchi oppure che quelle più piccole non sono coscienti dei problemi legati alla sicurezza per mancanza di competenze.

5 Strumento di analisi dinamica dei dati

L'incrocio di risultati di domande diverse può mettere in evidenza informazioni che ad una prima lettura non risultano visibili.

In questo documento sono presenti alcuni di queste combinazioni, ma per chi volesse esaminare ulteriori incroci di risultati è stato sviluppato uno strumento di analisi dinamica dei dati che permette, in forma grafica e in forma tabellare, di esaminare le relazioni tra le varie risposte.

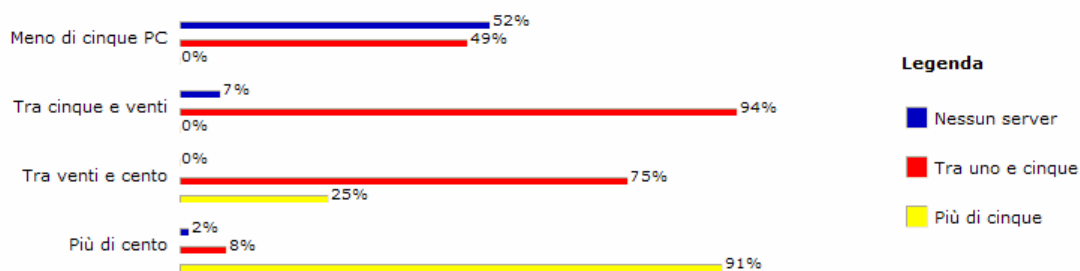
Lo strumento di analisi dinamica è disponibile nel sito isi.dti.supsi.ch e si presenta come nell'immagine seguente :



Sicurezza informatica e utilizzo dei computer in azienda - analisi dinamica dei dati

Questa pagina permette di esaminare in modo dinamico le risposte dell'inchiesta, sia direttamente per ogni domanda, sia confrontando in modo incrociato le differenti domande tra loro.

Per ulteriori informazioni sull'inchiesta si rimanda al documento ["Sicurezza informatica e utilizzo dei computer in azienda"](#)



Quanti PC sono presenti nella vostra azienda?

Ricalcola il grafico

Quanti server centrali sono presenti nella vostra azienda?

Inverti il grafico

- Percentuale relativa alla categoria di risposta
- Percentuale relativa al totale delle risposte

	Meno di cinque PC	%	Tra cinque e venti	%	Tra venti e cento	%	Più di cento	%
Nessun server	58	51.79	9	6.87	0	0	1	1.56
Tra uno e cinque	54	48.21	122	93.13	36	75	5	7.81
Più di cinque	0	0	0	0	12	25	58	90.63
% per risposta	112	100	131	100	48	100	64	100

La parte superiore mostra la rappresentazione grafica mentre nella parte inferiore vi è la presentazione tabellare.

Tra le due aree vi sono i menù a tendina che permettono di impostare le singole domande o le combinazioni di due domande.

Il calcolo delle percentuali può essere fatto rispetto alla categoria di risposta o al totale delle risposte. È possibile invertire il grafico in modo da avere una visione grafica differente per gli stessi dati.

6 Glossario

Botnet

Una rete di computer infettati da virus e cavalli di troia che può essere comandati a distanza da un'organizzazione all'insaputa dei proprietari.

Catena di Sant'Antonio

Messaggio di posta elettronica che viene distribuito con l'invito di diffonderlo ad altri e che descrive un improbabile tipo di proposta economica o annuncio di rischio o pericolo o altro.

Cavalli di Troia

Programmi che eseguono di nascosto operazioni nocive, camuffandosi in applicazioni e documenti utili per l'utente.

Cybercrime

Crimine informatico o crimine commesso utilizzando il computer, specialmente su Internet.

Chattare

Un modo di comunicare in tempo reale tramite Internet con più persone in un ambiente virtuale.

Codice malefico

Programma creati al solo scopo di causare danni più o meno estesi sui computer su cui viene eseguito. Si distinguono molte categorie, fra le più note: Virus, Spyware, Cavalli di Troia.

Firewall

Dispositivo hardware o applicazione software che hanno lo scopo di proteggere la rete locale da accessi non autorizzati, bloccando le porte con cui un sistema comunica all'esterno.

Instant messaging

vedi Chattare

Malware

vedi Codice Malefico

Password

Un insieme di caratteri o una parola chiave usata da un utente per autenticarsi, verificando l'identità e permettendo l'accesso a un computer o a una rete.

Personal firewall

Applicazione software con lo scopo di proteggere il PC da accessi non autorizzati, proteggendo le porte con cui un sistema comunica all'esterno.

PC

Personal Computer.

Social engineering

Tecnica di inganno che sfrutta la disponibilità, la buona fede e l'insicurezza delle persone per accedere per esempio a dati confidenziali o per indurre le vittime a effettuare determinate operazioni.

Spam

Invio massiccio di messaggi di posta elettronica di carattere pubblicitario, commerciale o inutile, senza alcuna preventiva richiesta da parte del destinatario. Possono contenere codice malefico.

Spyware

Programma che raccoglie informazioni riguardanti l'attività online o dati personali di un utente, trasmettendoli ad un'organizzazione che le utilizzerà per trarne profitto.

Virus

Codice informatico che si autoreplica attraverso programmi, messaggi di posta elettronica ecc. Può danneggiare i programmi e le informazioni contenute su PC e periferiche.

Webmail

Possibilità di accedere alla posta elettronica utilizzando il solo browser Web e scavalcando i normali sistemi di posta aziendale.

7 Riferimenti

ATED/SUPSI, *Studio ICT Ticino*, 2007

www.ated.ch / www.supsi.ch

Center for Security Studies - ETH, *Sicurezza dell'informazione nelle imprese svizzere*, agosto 2006,

www.melani.admin.ch/dokumentation/00123/00125/?lang=it

Computer Security Institute CSI – Federal Bureau of Investigation (FBI), *Computer Crime and Security Survey*, 2006,

www.gocsi.com

Department of Trade and Industry, *Information Security Breaches survey*, 2006

www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), *Rapporti semestrali*, 2005/2006,

www.melani.admin.ch/dokumentation/00123/00124/index.html?lang=it

InfoSurance, *Accroître la sécurité informatique des PME*, 2005,

www.infosurance.ch/fr/pdf/Brochure%20PME%2010%20points-2006-01-06.pdf

Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), *Raising Awareness in Information Security*, 2005

enisa.europa.eu/doc/pdf/deliverables/enisa_cd_awareness_raising.pdf

8 Appendice – Formulario di inchiesta

1. Quale è il vostro settore di attività?

- Commercio
- Produzione
- Servizi finanziari
- Sanità e salute
- Ente pubblico
- Settore legale
- Altro

2. Quanti PC sono presenti nella vostra azienda?

- Meno di cinque
- Tra cinque e venti.
- Tra venti e cento
- Più di cento

3. Quanti server centrali sono presenti nella vostra azienda?

- Nessuno
- Tra uno e cinque.
- Più di cinque

4. Esiste un collegamento Internet in azienda?

- No
- Sì, via modem
- Sì, permanente (ADSL, linea affittata)

5. Tutti i PC aziendali hanno accesso a Internet?

- Sì
- No

6. In che misura viene utilizzata la rete Internet in azienda?

- molto normale poco per la posta elettronica (comunicazione con clienti, fornitori, ecc.)
- molto normale poco per ricercare informazioni necessarie per l'attività lavorativa
- molto normale poco per attività amministrative e commerciali (telebanking, acquisti)
- molto normale poco per promuovere i vostri prodotti/servizi
- molto normale poco per altre attività

7. La posta elettronica viene usata per inviare/ricevere documenti importanti o riservati?

- Sì
- No

8. Siete al corrente di quali informazioni devono essere protette per legge?

- I dati delle persone
- I dati dell'azienda
- Non saprei

9. Ci sono informazioni critiche sui PC e sui server aziendali? (scelta multipla possibile)

- Sì, informazioni tutelate dalla legge sulla protezione dei dati
- Sì, informazioni riservate dell'azienda (strategie, contratti, progetti, ecc.)
- Sì, informazioni operative dell'azienda (contabilità, ordini, fatture, ecc.)
- No
- Non saprei

10. Quale danno potrebbe derivare da una distruzione o da una perdita di queste informazioni critiche?

- Nessun danno per l'azienda
- Danno moderato per l'azienda
- Danno grave per l'azienda

11. Quale danno potrebbe derivare da un furto o da una diffusione pubblica di queste informazioni critiche?

- Nessun danno per l'azienda
- Danno moderato per l'azienda

Danno grave per l'azienda

12. Quali sono le competenze dei dipendenti nell'uso dei PC e di Internet?

- Molto buone, hanno seguito dei corsi
- Buone, hanno un'esperienza di lavoro che permette di adeguarsi alle situazioni
- Normali, conoscono quello che serve per fare il loro lavoro
- Deboli, spesso non sono in grado di svolgere delle attività e devono chiedere ad altri

13. Avete delle esigenze di controllo dei dipendenti nell'uso dei PC e di Internet nella vostra azienda?

- Si
- No

14. Quali di queste attività ritenete che siano gravi nell'utilizzo dei PC da parte dei dipendenti? (scelta multipla possibile)

- Usare la posta elettronica per messaggi privati
- Consultare occasionalmente siti informativi di giornali, sport, viaggi, ecc.
- Consultare regolarmente siti informativi di giornali, sport, viaggi, ecc.
- Consultare occasionalmente siti di dubbia moralità, gioco d'azzardo, ecc.
- Consultare occasionalmente siti su offerte di lavoro, opportunità di guadagno, ecc.
- Chattare con persone all'esterno dell'azienda
- Altro

15. Avete dei regolamenti che disciplinano l'uso dei PC e di Internet per i dipendenti?

- Si
- No
- In parte

16. Quali di queste misure di sicurezza avete previsto per la vostra infrastruttura informatica? (scelta multipla possibile)

- Antivirus su tutti i PC
- Antispyware su tutti i PC
- Antispam su tutti i PC
- Personal firewall su tutti i PC
- Firewall centralizzato
- Gruppo di continuità elettrica per i server
- Salvataggio giornaliero dei dati
- Password di accesso ai PC
- Nessuna misura particolare
- Non sono al corrente delle misure previste
- Altro

17. Vengono fatti gli aggiornamenti degli antivirus e del software di sistema?

- Regolarmente
- Ogni tanto
- Mai

18. Vi preoccupano particolari problemi di sicurezza nell'uso dei PC e di Internet?

- No
- Si, quali

19. Esiste un responsabile della sicurezza informatica in azienda?

- Si
- No

Azienda

Persona di contatto

Posta elettronica

Le informazioni raccolte vengono trattate in modo
confidenziale e non saranno comunicate a terzi.
© 2006, S. Marioni, SUPSI