Direttiva sulla sicurezza delle informazioni

amag

Indice

1. Introduzione.

Questa direttiva viene applicata a tutto il gruppo AMAG e ai suoi collaboratori, nonché a terzi che conservano o elaborano le informazioni del gruppo AMAG o che le rilevano per conto del gruppo. Le parti terze devono essere vincolate contrattualmente alla presente direttiva oppure devono presentare una dichiarazione comprensibile e verificabile, in cui viene specificato che anch'esse sono soggette e devono rispettare una direttiva analoga. In seguito si utilizzerà il termine «collaboratori» per i dipendenti del gruppo AMAG e i collaboratori di parti terze.

Le misure di sicurezza qui descritte proteggono i collaboratori (e le parti terze nel senso sopraindicato) e i clienti del gruppo AMAG, nonché i visitatori, da attacchi interni ed esterni. Le presenti prescrizioni contribuiscono inoltre a proteggere i beni materiali e immateriali del gruppo AMAG, nonché ad adempiere alle direttive di legge.

2. Principi fondamentali.

La seguente lista riepiloga e illustra, in generale, i principi fondamentali della sicurezza delle informazioni all'interno del gruppo AMAG.

1. Tutti i collaboratori del gruppo AMAG sono responsabili della sicurezza delle informazioni nell'ambito dei loro compiti e delle loro attività. Rispettando la presente direttiva, i collaboratori si assumono le propria responsabilità.
2. Deve sempre essere garantito che i dati da elaborare o trasferire siano accessibili solo a persone autorizzate. Bisogna inoltre accertarsi che venga tutelata la riservatezza quando vengono assegnati dei diritti, sia di lettura che di scrittura (principio «need to know» e «need to do»). La probabilità che dati confidenziali raggiungano destinazioni sbagliate aumenta proporzionalmente al numero dei destinatari.
3. Quando si utilizzano strumenti informatici, i dati memorizzati, elaborati o utilizzati in altro modo devono essere trattati in base alla corrispondente necessità di protezione. Deve essere in particolare modo evitato che persone non autorizzate entrino in possesso di dati confidenziali o dati personali.
4. Non si devono utilizzare supporti informatici sconosciuti, come ad esempio chiavette USB trovate per caso. I supporti informatici sconosciuti che si sono trovati nei locali o sulle superfici aziendali del gruppo AMAG devono essere consegnati ai responsabili del reparto informatico indicando il luogo e l'ora del ritrovamento.
5. Internet va utilizzato con cautela, soprattutto se non si conoscono i servizi offerti o se sono chiaramente dubbiosi. La protezione da malware e la prevenzione da danni alla reputazione hanno la massima priorità.
6. Per evitare, il più possibile, infiltrazioni di malware, si possono filtrare le connessioni a Internet del gruppo AMAG (web, e-mail, chat ecc.) per bloccare i contenuti indesiderati o addirittura pericolosi. Questi filtri funzionano ai sensi delle disposizioni della legge svizzera sulla protezione dei dati. Non ha luogo un'analisi di routine di come i collaboratori utilizzano Internet.
7. Gli allegati alle e-mail possono essere aperti solo se provenienti da mittenti conosciuti. In caso di

dubbi informare gli addetti alla sicurezza informatica.

8. Le password sono individuali, personali e non devono essere rese note.
9. Chiavi personali, badge (KABA) ecc. non devono essere consegnati a terzi, nemmeno se questi sono membri del proprio team.
10. Le chiavi o i badge (KABA) non personali, ad. esempio le chiavi generali per i magazzini, possono essere consegnate solo a persone autorizzate. In caso di dubbi va chiarito presso il proprio superiore chi sono le persone autorizzate. L'utilizzo di chiavi o badge non personali deve essere protocollato, indicando il nome di chi ne prende possesso, la data e la durata dell'utilizzo e il tipo di chiave.
11. Non devono essere trasmesse informazioni commerciali a persone sconosciute o non autorizzate. Questo vale tanto per la comunicazione orale, quanto per la consegna o la trasmissione tramite e-mail, chiavette USB, altri supporti elettronici, stampa o modi analoghi.
12. Se non si è sicuri che una determinata persona sia autorizzata ad accedere o ricevere dei dati, bisogna chiarire con il proprio superiore se glielo si può consentire.
13. Non si deve permettere che persone sconosciute si trattengano nelle zone non pubbliche. Questo vale per le zone non pubbliche di edifici, aree transennate, capannoni ecc.
14. I visitatori di ditte terze devono essere annunciati in anticipo e registrati in un elenco dei visitatori, se vengono fatti accedere a zone non pubbliche.
15. Bisogna fare attenzione a non parlare di informazioni riservate quando ci si trova in spazi pubblici e soprattutto, ma non solo, sui mezzi di trasporto pubblici, in ristoranti ecc. Specialmente durante pranzi o cene di affari, bisogna stare attenti a che le informazioni confidenziali non possano essere ascoltate dai tavoli vicini.

3. Password, chiavi ecc.

Password, chiavi ecc. permettono l'accesso a sistemi, dati e quindi a informazioni. L'utilizzo corretto di password, chiavi per porte, portoni, casseforti ecc. è quindi di rilevante importanza per tutti gli obiettivi di sicurezza.

3.1 Password.

Le password personali non devono essere rese note né ai membri del team, né agli assistenti informatici interni o esterni e neppure ad altri gruppi di persone. Se si sospetta, che una password sia stata scoperta, la si deve modificare immediatamente.

Quando si seleziona una password è necessario attenersi a tutti i requisiti in merito indicati nei sistemi. Si consiglia, per quanto possibile, di scegliere una password piuttosto lunga, una cosiddetta «passphrase» (una frase d'accesso, invece di una parola d'accesso).

Una passphrase può essere composta, ad esempio, da una combinazione di abbreviazioni, intere parole e cifre, al posto di semplici lettere. Se qualcuno si interessa di fotografia, la frase completa potrebbe essere: «La fotografia è il mio hobby!» e due delle tante conversioni in passphrase potrebbero essere

«Foèmioho0661!» oppure «Foto4everperme.». È logico che le due passphrase qui indicate non devono essere utilizzate.

3.2 Badge.

Negli ambienti in cui vengono utilizzati i badge, questi non devono essere consegnati ad altri collaboratori, a collaboratori di parti terze o a visitatori.

L'utilizzo di badge non personali deve essere protocollato, indicando il nome di chi ne prende possesso, la data e la durata dell'utilizzo e il tipo di badge.

3.3 Chiavi fisiche.

Con chiavi fisiche si intendono, nella presente direttiva, le normali chiavi, come quelle che si utilizzano generalmente per ingressi, porte e, a volte anche per casseforti.

Le chiavi fisiche personali non devono essere consegnate ad altre persone. Devono essere conservate sempre in modo sicuro, come ad esempio portandosele dietro.

Le chiavi che vengono utilizzate da più persone, ad esempio da tutto un team, devono essere custodite, durante la notte, in una cassaforte protetta da combinazione numerica oppure essere portate a casa dalla persona responsabile.

L'utilizzo di chiavi fisiche non personali deve essere protocollato, indicando il nome di chi ne prende possesso, la data e la durata dell'utilizzo e il tipo di chiave.

4. Utilizzo di strumenti informatici.

I dispositivi elettronici (notebook, smartphone ecc.) che il gruppo AMAG mette a disposizione dei collaboratori, così come i programmi e i dati, sono destinati a un uso professionale e devono essere utilizzati con cura (evitarne il furto, la distruzione, l'accesso da parte di apparecchi terzi ecc.). Gli apparecchi incustoditi devono essere disabilitati. È autorizzato l'utilizzo di dispositivi elettronici e software privati (ad esempio telefoni cellulari) non forniti dal gruppo AMAG, a cui vengono però anche applicate le misure di prudenza sopracitate.

Bisogna essere altrettanto vigili quando si utilizza Internet e i suoi servizi; si veda in merito anche il capitolo «Internet, social media, chat, e-mail».

Per proteggersi dalla «social engineering» (attività di manipolazione sociale) bisogna fare attenzione a non rendere note informazioni riservate a persone non chiaramente identificabili comunicandole per telefono, in conversazioni dirette o tramite altri canali (e-mail, chat ecc.).

I dati che non sono più necessari, cioè i dati non servono più a fini commerciali e che non sottostanno per legge a un obbligo di conservazione (ad esempio le pure e-mail interne), devono essere cancellati o rimossi. Lo stesso vale per i dati su carta.

5. Internet, social media, chat, e-mail.

Internet deve essere utilizzato, in primo luogo, a scopi di lavoro. Se usato in modo ragionevole, ci se ne può servire anche a fini privati. Sono cioè permessi, nell'ambito dell'utilizzo personale, e-mail, altri servizi di comunicazione e social network, chat, blog. L'utilizzo dei mezzi di comunicazione a scopi privati non deve pregiudicare l'attività lavorativa dei collaboratori. Bisogna tenere conto che le informazioni non possono più essere rimosse, o solo molto difficilmente, da Internet.

La comunicazione nell'ambito delle pubbliche relazioni è invece compito del reparto addetto, che è l'unico autorizzato a pubblicare informazioni ufficiali a nome del gruppo AMAG sui canali pubblici (siti web, Twitter, Facebook ecc.). Un'eventuale necessità di comunicazione deve essere discussa con il Group Communication.

Nonostante i suoi vari vantaggi, Internet permette purtroppo anche la diffusione di qualsiasi tipo di malware, come virus, trojan, e-mail per phishing ecc. Il malware viene normalmente trasmesso attraverso siti web o e-mail infette. Nonostante AMAG filtri le e-mail in entrata per rilevare la presenza di malware, si possono tuttavia ricevere singole e-mail contenenti malware, inserito in particolare negli allegati. Stare particolarmente attenti nell'aprire e-mail inviate da mittenti sconosciuti o che contengono espressioni più «insolite» del dovuto. Aprire e-mail o allegati contenenti malware può provocare danni ingenti nonostante i programmi di protezione presenti (software antivirus). Se si sospetta la presenza di malware, comunicarlo immediatamente scrivendo a it-systems.network@amag.ch

6. Protezione fisica.

Questo capitolo descrive i principi della protezione fisica. L'obiettivo principale è proteggere le persone che si trovano sulle superfici e negli edifici del gruppo AMAG, nonché tutti gli immobili, gli utensili, le macchine, le scorte di magazzino, le attrezzature per l'ufficio, qualsiasi apparecchiatura informatica e tutti gli altri valori del gruppo AMAG.

6.1 Principi introduttivi.

L'ingresso alle aree, agli edifici e alle zone interne degli stessi che non sono accessibili al pubblico può essere concesso solo alle persone autorizzate e che ne hanno bisogno per svolgere la loro attività (principio «need to know» e soprattutto «need to do»).

6.2 Portoni e porte.

Porte e passaggi che dividono zone diverse, come ad esempio uffici, garage o magazzini, possono essere equipaggiati con ulteriori meccanismi di sicurezza. Questi meccanismi di protezione non devono essere scardinati. Le chiavi o i badge non devono, ad esempio, essere consegnati a persone non autorizzate e soprattutto non ai visitatori. Le chiavi personali o i badge non devono assolutamente essere dati ad altre persone.

6.3 Responsabilità.

Il rispettivo addetto alla sicurezza in loco è responsabile della protezione fisica. L'addetto alla sicurezza garantisce che le misure di sicurezza per la realizzazione della presente direttiva siano sufficienti e

consoni alle esigenze concrete dei rispettivi ambienti. Se occorre, l'addetto alla sicurezza organizza verifiche finalizzate a tale scopo.

L'addetto alla sicurezza è responsabile che siano state adottate le misure di sicurezza fisica necessarie. In caso di bisogno, l'addetto alla sicurezza può ricevere consulenza su queste tematiche.

7. Visitatori.

Ai sensi della presente direttiva sono considerati visitatori tutti coloro che non sono collaboratori del gruppo AMAG e che non hanno un posto di lavoro permanente all'interno del gruppo AMAG. Quanto qui di seguito esposto viene applicato alle zone non pubbliche. Gli showroom o le mense aperte al pubblico non fanno parte di quanto qui esposto.

I visitatori devono essere precedentemente annunciati da parte di un collaboratore con posto di lavoro permanente all'interno del gruppo AMAG e registrato nella lista dei visitatori della rispettiva sede indicando il suo nome, la ditta, la data e il motivo della visita. La persona che si presenta quale ospitante della visita è anche responsabile per il visitatore.

8. Monitoraggio.

Lo scopo del monitoraggio è la protezione dei dati e dell'infrastruttura informatica. Possono essere utilizzati filtri anti-malware per la protezione da siti web pericolosi e diffusori di malware o contro server il cui utilizzo potrebbe rappresentare un problema per la reputazione. Il monitoraggio deve inoltre individuare gli attacchi all'ambiente del gruppo AMAG provenienti da Internet e da Intranet.

Non viene monitorato periodicamente l'utilizzo di Internet dei singoli collaboratori. Il gruppo AMAG si attiene alla legge svizzera sulla protezione dei dati personali.

9. Allegato: definizione di informazioni e dati.

Stampa	**Definizione nel quadro della presente direttiva**	**Esempi**
Dati	Informazione su un supporto dati o mezzo di trasporto	Stampe su carta/file/e-mail/siti web/ecc.
Informazione	La dichiarazione stessa/il contenuto	Notizia/dichiarazione/direttiva/descrizione

Validità

Autore	AMAG Informatica

Versione	Data	Motivo dell'elaborazione	Autore
1.0	23.10.2019	Prima redazione	Information Technology Services