**Information Security**

Analisi e trattamento del rischio di un’azienda informatica per lo sviluppo software, web hosting e data center



WebSoft nasce nel 2004 dall’esperienza pluriennale di un gruppo di professionisti che operano da anni a Torino nel settore dell’Information Tecnology. WebSoft si propone come azienda qualificata nella consulenza, progettazione e realizzazione di progetti informatici legati all’infrastruttura tecnologica e all’integrazione di sistemi e tecnologie, mettendo a disposizione risorse, esperienza, entusiasmo, know-how tecnico e commerciale.

L’obbiettivo principale dell’azienda è fornire alle varie imprese e privati consulenza, servizi e soluzioni integrate per la gestione dell'infrastruttura e dei contenuti informatici. Infine WebSoft, offre servizi di hosting web-based e archiviazione dati.

****

**CONTESTO DELL’AZIENDA**

|  |  |
| --- | --- |
| Interno:   * Server dedicati per i servizi di hosting e data center * Dipendenti dell’azienda e loro relative conoscenze * Dispositivi per lo sviluppo software * Personale:   + 1 Project Manager (CEO)   + 1 impiegato amministrativo   + 4 programmatori | Esterno:   * Richiesta di sviluppo di applicativi e spazi di archiviazione per grandi imprese * Richiesta di sviluppo di applicativi per medie e piccole imprese * Relazioni con i vari fornitori di server e in generale dispositivi informatici * Relazioni con vari ISP (per web hosting) |

INFORMAZIONI DA PROTEGGERE

* Dati sensibili dei clienti
* Codice sorgente in fase di sviluppo
* Server di hosting e data center
* Credenziali d’accesso ai vari dispositivi
* Dispositivi dei dipendenti in sede e da remoto

MINACCE

* Esfiltrazione/manomissione dei dati dei clienti
* Esfiltrazione/manomissione del codice sorgente
* Manomissione dei computer dei dipendenti
* Attacchi hacker verso i server aziendali (non intromissione)
* Intromissione di un terzo all’interno di un dispositivo utilizzato in azienda o per telelavoro
* Spionaggio industriale (assunzione personale con intenzioni fraudolente)
* Scarsa formazione del personale
* Intrusione da parte di terzi all’interno di un’area ad accesso privilegiato
* Furto di identità da parte di terzi (compromissione di chiavi crittografiche relative a uno o più domini di hosting)
* Accesso non autorizzato ad un’area protetta non esposta alla rete Internet
* Furto o manipolazione di dati sensibili o informazioni presenti su dispositivi dismessi o riutilizzati
* Accesso non autorizzato a dispositivi lasciati incustoditi degli utenti
* Perdita o corruzione di dati causata da software non aggiornato
* Perdita dei dati dei clienti/dei codici sorgenti per mancato backup preventivo
* Infezione da malware
* Navigazione su siti malevoli

CRITERIO VALUTAZIONE PROBABILITA’

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | *Molto Raro* | *Raro* | *Improbabile* | *Possibile* | *Frequente* | *Quasi certo* |
| *Livello* | *1* | *2* | *3* | *4* | *5* | *6* |
| *Probabilità* | *Ogni 10 anni* | *Ogni 5 anni* | *Ogni 2 anni* | *Ogni 6 mesi* | *Ogni mese* | *Ogni settimana* |

CRITERIO VALUTAZIONE IMPATTO

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | *Molto Basso* | *Basso* | *Medio* | *Alto* | *Molto Alto* |
| *Livello* | *1* | *2* | *3* | *4* | *5* |
| *Impatto* | *Fino a 5k euro* | *Tra 5k a 20k euro* | *Tra 20k a 35k euro* | *Tra 35k e 50k euro* | *Più di 50k euro* |

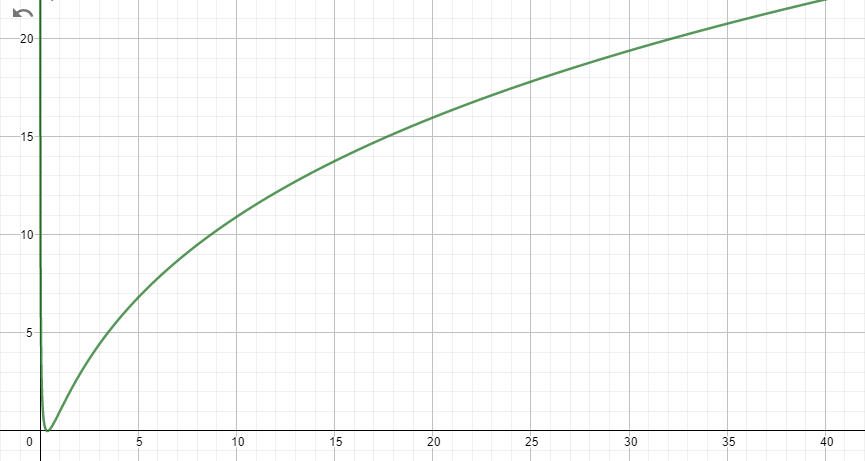
MATRICE DI CALCOLO DEL RISCHIO

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | *Molto Raro* | *Raro* | *Improbabile* | *Possibile* | *Frequente* | *Quasi certo* |
| *Molto Alto* | *7* | *11* | *14* | *16* | *18* | *20* |
| *Alto* | *6* | *9* | *12* | *14* | *16* | *17* |
| *Medio* | *4* | *8* | *10* | *12* | *14* | *15* |
| *Basso* | *3* | *6* | *8* | *9* | *11* | *12* |
| *Molto Basso* | *1* | *3* | *4* | *6* | *7* | *9* |

LIVELLI DI RISCHIO

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Basso* | *Medio-Basso* | *Moderato* | *Medio-Alto* | *Alto* |

FUNZIONE PER IL CALCOLO DEL RISCHIO

**

ANALISI DELLE MINACCE

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | ***Probabilità*** | ***Impatto*** | ***Rischio*** | ***Da trattare*** |
| *Esfiltrazione/manomissione*  *dei dati dei clienti* | *Possibile* | *Molto-Alto* | *Alto* | *X* |
| *Esfiltrazione/manomissione del codice sorgente* | *Possibile* | *Alto* | *Medio-Alto* | *X* |
| *Manomissione dei computer dei dipendenti* | *Improbabile* | *Molto-Alto* | *Medio-Alto* | *X* |
| *Attacchi hacker verso i server aziendali (non intromissione)* | *Possibile* | *Alto* | *Media-Alto* | *X* |
| *Intromissione di un terzo all’interno di un dispositivo utilizzato in azienda o per telelavoro* | *Raro* | *Molto-Alto* | *Medio-Alto* | *X* |
| *Spionaggio industriale (assunzione personale con intenzioni fraudolente)* | *Molto-Raro* | *Alto* | *Medio-Basso* |  |
| *Scarsa formazione del personale* | *Improbabile* | *Alto* | *Medio-Alto* | *X* |
| *Intrusione da parte di terzi all’interno di un’area ad accesso privilegiato* | *Raro* | *Molto-Alto* | *Medio-Alto* | *X* |
| *Furto di identità da parte di terzi (compromissione di chiavi crittografiche relative a uno o più domini di hosting)* | *Molto-Raro* | *Molto-Alto* | *Moderato* |  |
| *Accesso non autorizzato ad un’area protetta non esposta alla rete Internet* | *Improbabile* | *Molto-Alto* | *Medio-Alto* | *X* |
| *Furto o manipolazione di dati sensibili o informazioni presenti su dispositivi dismessi o riutilizzati* | *Improbabile* | *Alto* | *Medio-Alto* | *X* |
| *Accesso non autorizzato* a dispositivi lasciati incustoditi dagli utenti | *Frequente* | *Alto* | *Alto* | *X* |
| *Perdita o corruzione di dati causata da software non aggiornato* | *Molto-Raro* | *Medio* | *Basso* |  |
| *Perdita dei dati dei clienti/dei codici sorgenti per mancato backup preventivo* | *Raro* | *Molto-Alto* | *Medio-Alto* | *X* |
| *Infezione da malware* | *Possibile* | *Molto-Alto* | *Alto* | *X* |
| *Navigazione su siti malevoli o in generale non consentiti* | *Quasi certo* | *Alto* | *Alto* | *X* |

P.S. Sono stati trattati tutti i rischi il cui valore risulta essere maggiore o uguale ad 11.

CONTROLLI DA ATTUARE

A.5 Politiche per la sicurezza delle informazioni

* A.5.1 Indirizzi della direzione per la sicurezza delle informazioni
  + A.5.1.1 Politiche per la sicurezza delle informazioni

A.6 Organizzazione della sicurezza delle informazioni

* 6.1 Organizzazione Interna
  + A.6.1.4 Contatti con gruppi specialistici
  + A.6.1.5 Sicurezza delle informazioni nella gestione dei progetti
* A.6.2 Dispositivi portatili e telelavoro
  + A.6.2.1 Politica per i dispositivi portatili
  + A.6.2.2 Telelavoro

A.7 Sicurezza delle risorse umane

* A.7.2 Durante l’impiego
  + A.7.2.2 Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni

A.8 Gestione degli asset

* A.8.2 Classificazione delle informazioni
  + A.8.2.1 Classificazione delle informazioni

A.9 Controllo degli accessi

* A.9.2 Gestione degli accessi degli utenti
  + A.9.2.1 Registrazione e de-registrazione degli utenti
  + A.9.2.3 Gestione dei diritti di accesso privilegiato
  + A.9.2.4 Gestione delle informazioni segrete di autenticazione degli utenti
  + A.9.2.6 Rimozione o adattamento dei diritti di accesso

A.9 Controllo degli accessi

* A.9.3 Responsabilità dell'utente
  + A.9.1.1 Politica di controllo accessi
  + A.9.1.2 Accesso alle reti e ai servizi di rete
* A.9.4 Controllo degli accessi ai sistemi e alle applicazioni
  + A.9.4.1 Limitazione dell’accesso alle informazioni
  + A.9.4.2 Procedure di log-on sicure
  + A.9.4.3 Sistema di gestione delle password
  + A.9.4.4 Uso di programmi di utilità privilegiati
  + A.9.4.5 Controllo degli accessi al codice sorgente dei programmi

A.11 Sicurezza fisica e ambientale

* A.11.2 Apparecchiature
  + A.11.2.6 Sicurezza delle apparecchiature e degli asset all’esterno delle sedi
  + A.11.2.7 Dismissione sicura o riutilizzo delle apparecchiature
  + A.11.2.8 Apparecchiature incustodite degli utenti

A.12 Sicurezza delle attività operative

* A.12.2 Protezione dal malware
  + A.12.2.1 Controlli contro il malware
* A.12.3 Backup
  + A.12.3.1 Backup delle informazioni
* A.12.5 Controllo del software di produzione
  + A.12.5.1 Installazione del software sui sistemi di produzione
* A.12.6 Gestione delle vulnerabilità tecniche
  + A.12.6.1 Gestione delle vulnerabilità tecniche
  + A.12.6.2 Limitazioni all’installazione del software

A.13 Sicurezza delle comunicazioni

* A.13.1 Gestione della sicurezza della rete
  + A.13.1.2 Sicurezza dei servizi di rete
* A.13.2 Trasferimento delle informazioni
  + A.13.2.1 Politiche e procedure per il trasferimento delle informazioni

A.18 Conformità

* A.18.1 Conformità ai requisiti cogenti e contrattuali
  + A.18.1.4 Privacy e protezione dei dati personali

PIANO DI TRATTAMENTO DEL RISCHIO

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rischio** | **Danni all’azienda** | **Rischio residuo** | **Situazione attuale** | **Strategia di mitigazione** |
| Esfiltrazione/manomissione dei dati dei clienti | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita tali dati) | Alto | Dati dei clienti presenti in un file excel di un dispositivo collegato alla rete Internet | Spostare i dati dei clienti in una directory (es. LDAP) in un dispositivo non collegato alla rete Internet ed accedibile solo attraverso un’autenticazione a due fattori (password + token).  Limitazione di accesso a tali dati, esclusivamente ad un ristretto gruppo di persone |
| Esfiltrazione/manomissione del codice sorgente | Furto di codice sorgente, calo della produttività causata dal tempo di recupero del lavoro perso | *Medio-Alto* | Codici sorgenti memorizzati sui vari dispositivi aziendali | Predisporre un sistema di versioning del software (es. GIT) per poter centralizzare, sincronizzare e proteggere i vari codici sorgenti |
| Manomissione dei computer dei dipendenti | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita di tali dati), calo della produttività causata dal tempo di recupero del lavoro perso | *Medio-Alto* | Ciascun dipendente può modificare i file di sistema del proprio dispositivo aziendale | I computer dei dipendenti dovranno essere dotati di software che limitano l’accesso a risorse del sistema e l’installazione di applicativi non consentiti. Tali software di controllo non potranno essere rimossi dai dispositivi se non da personale autorizzato |
| Attacchi hacker verso i server aziendali (non intromissione) | Perdita di informazioni, disservizio nei confronti dei clienti, calo della produttività causata dal tempo di recupero del lavoro perso | *Media-Alto* | Rete locale non protetta da firewall o packet filter. Porte aperte verso alcuni dispositivi “critici”. | Installare un firewall sul gateway che si interfaccia alla rete Internet ed eventualmente anche nei dispositivi aziendali.  Chiudere determinate porte inutilizzate aperte del gateway per escludere eventuali vulnerabilità |
| Intromissione di un terzo all’interno di un dispositivo utilizzato in azienda o per telelavoro | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita di tali dati) | *Medio-Alto* | Dispositivi aziendali e non protetti da password deboli | Comunicare al personale la “debolezza” della password attuale incoraggiandolo ad utilizzarne una più sicura dal punto di vista della sicurezza.  Proteggere l’accesso ai dispositivi da remoto attraverso riconoscimento IP e autenticazione basata su password. |
| Scarsa formazione del personale | Perdita parziale dei dati relativi ai codici sorgenti (ad esempio per mancato salvataggio), autorizzazione inconsapevole di programmi malevoli all’interno del dispositivo | Medio-Alto | Personale scelto in solamente base in base alle competenze pregresse. | Verificare accuratamente le competenze pregresse del dipendente ed istruirlo riguardo l’utilizzo e l’accesso ai dispositivi aziendali in sede e da remoto |
| Intrusione da parte di terzi all’interno di un’area ad accesso privilegiato | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita di tali dati) | Medio-Alto | Dispositivi appartenenti ad un’area ad accesso privilegiato (contenenti informazioni sensibili, quali ad esempio i dati dei clienti) protetti solamente da autenticazione basata su password | Circoscrivere le aree ad accesso privilegiato attraverso un sistema di autenticazione a due fattori (sempre basate su password e autenticazione fisica basata su token). Limitare il possedimento di tali credenziali ad un numero ristretto di persone, mitigando quindi la divulgazione di tali credenziali d’accesso a terzi |
| Furto o manipolazione di dati sensibili o informazioni presenti su dispositivi dismessi o riutilizzati | Diffusione delle credenziali, dei dati d’accesso, dei codici sorgenti dei progetti e delle informazioni contenute nei dispositivi dismessi | Medio-Alto | Dismissione superficiale dei dispositivi aziendali.  Parziale cancellazione delle informazioni contenute in essi | Ripulire sempre i dispositivi prima del loro riutilizzo o dismissione attraverso software di formattazione del disco rigido. Se tali dispositivi devono, per qualche motivo, essere dismessi, adottare tecniche specializzate di distruzione come ad esempio la punzonatura |
| Accesso non autorizzato a dispositivi lasciati incustoditi dagli utenti | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita di tali dati) | Alto | Dispositivi lasciati completamente incustoditi durante il periodo nel quale il proprietario è assente | Adottare o incrementare il controllo sui dispositivi lasciati incustoditi in sede. Esortare il personale a non lasciare incustodito il loro dispositivo durante il lavoro da remoto. Utilizzare delle tecniche di cifrature del disco quando il dispositivo non è in uso |
| Perdita dei dati dei clienti/dei codici sorgenti per mancato backup preventivo | Cause legali da parte dei clienti, calo della produttività causata dal tempo di recupero del lavoro perso | Medio-Alto | Backup effettuati in intervalli di tempo eccessivamente lunghi. Supporti di backup facilmente accedibili e leggebili. | Effettuare periodicamente uno o più backup dei dati dei clienti/dei codici sorgenti. Proteggere fisicamente tali backup e cifrarne il contenuto per scongiurare copie non consentite |
| Infezione da malware | Furto e perdita di informazioni, cause legali da parte dei clienti (nel caso di perdita di tali dati), proporzionale calo della produttività causata dal tempo di ripristino del dispositivo | Alto | Dispositivi dotati di software anti-malware obsoleto o mancante. Personale poco istruito riguardo i possibili danni causati da software potenzialmente malevolo | Installare sui dispositivi in sede o da remoto del software anti-malware aggiornato. Istruire il personale riguardo le possibili infezioni causate da software malevolo e sui possibili accorgimenti da adottare per evitare tali infezioni |
| Navigazione su siti malevoli o in generale non consentiti | Calo della produttività del dipendente, problemi legali in generale, installazione di software non consentito | Alto | Ciascun dipendente può navigare in Internet senza limitazioni di alcun tipo | Configurare i dispositivi in sede o da remoto in modo tale da evitare che il personale acceda a domini non consentiti (ad esempio utilizzando un proxy server che filtri le richieste HTTP). Tale configurazione non potrà essere modificata se non da personale autorizzato |