Cyber MSME

Cybersecurity per Micro, Piccole e Medie imprese

Crisis management — Mi hanno hackerato, cosa fare?

By CTS Customized Training Solutions & CASE

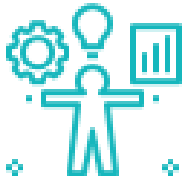
Erasmus+

Obiettivi e risulatati:

Alla fine di questo modulo sarai in grado di:

- Identificare una crisi informatica
- Identificare potenziali rischi e mancanze
- Evitare gli errori più comuni durante una crisi informatica
- Creare o migliorare il tuo piano di gestione di una crisi
- Prepararti per saper rispondere adeguatamente ed essere in grado di ripristinare le attività dopo una crisi

Index



Unità 1: **Gestione di una crisi informatica**

Unità 2: **Rispondere a una crisi informatica**

Unità 3: **Riprendersi da una crisi informatica**

Unità 1: Gestione di una crisi informatica

Sezione 1.1: Perchè è necessario gestire una crisi?

Se gestisci una PMI, probabilmente non hai abbastanza risorse finanziarie e umane per prevenire e fronteggiare delle crisi informatiche.
In caso di una media impresa, è più realistico che riesca a delegare tale compito a professionisti esterni. Tuttavia, anche le micro e piccole imprese dovrebbero sentirsi quasi obbligate ad investire per il miglioramento della sicurezza online.
Il protocollo da seguire in caso di crisi informatica si suddivide in 3 steps:

1) prevenzione;

2) risposta alla crisi;

3) recupero.

In particolare, in questo modulo affronteremo i primi due steps.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unità 1: Gestione di una crisi informatica

Sezione 1.2: Identificare la crisi

Prima di tutto, dobbiamo conoscere le varie tipologie di crisi informatica

Una crisi informatica è qualsiasi tipo di evento che influenza negativamente la tua attività

Per esempio:

- Hackeraggio dei devices
- screen mirroring dei tuoi devices
- Email duplicate
- Furto di informazioni bancarie
- Furto del database clienti
- Sito web no funzionante
- Violazione della rete
- Negazione di servizio, etc.

Unità 1: Gestione di una crisi informatica

Sezione 1.2: Identificare una crisi

Tutti gli eventi informatici potenzialmente sospetti dovrebbero comportare l'attivazione del protocollo da seguire e l'immediata attuazione della fase 2 – la risposta- anche quando non si è certi al 100% di ciò che sta accadendo.

RICORDA! Non si tratta solo di te e della tua attività, ma devi tenere conto anche di:

- La sicurezza dei tuoi cleinti e dei tuoi partner
- Il profitto dell'attività
- La reputazione aziendale

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unità 2: Rispondere ad una crisi informatica

Sezione 2.1: Il ruolo del tempo

La tua reazione in caso di crisi informatica deve essere veloce.

Delle volte, hai pochi secondi per decidere cosa fare e non puoi permetterti di andare in panico, potresti rovinare il lavoro di una vita!

Gli errori più comuni commessi dalle PMI durante una crisi informatica sono:

- Non dominare delle persone responsabili per la gestione della crisi
- Non avere a portata di mano i contatti del fornitore
- Non programmare un protocollo comunicativo

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unità 2: Rispondere a una crisi informatica

Sezione 2.1: Il ruolo del tempo

Perchè è necessario delegare dei responsabili?

Rispondere adeguatamente a una crisi informatica significa prendere qualsiasi provvedimento per gestire l'evento critico e fornire aggiornamenti agli stakeholders.

Rispondere ad una crisi informatica significa pianificare preventivamente le azioni da fare.
Questo perché, in caso di attacco, non c'è tempo per pensare cosa fare.
È importante essere preparati e delegare dei responsabili!

Cosa ne pensi ?: I responsabili dovrebbero avere delle conoscenze pregresse in ambito IT o no?

Erasmus+

Unità 2: Rispondere a una crisi informatica

Sezione2.1: Il ruolo del tempo

Non sai se le persone a cui deleghi il compito di gestire la crisi informatica debbano avere delle conoscenze pregresse in ambito IT? Dunque, ti possiamo dire che non è il fattore più importante da valutare. Perché?
Innanzitutto, capiamo quali sono le responsabilità di queste figure:

- Sapere come fare il backup di un piano
- Saper monitorare tutte le attività durante la crisi
- Guidare la strategia interna
- Implementare il protocollo comunicativo in caso di crisi

Erasmus+

Unità 2: Rispondere a una crisi

Sezione 2.1: Il ruolo del tempo

Se la persona delegata per la gestione di una crisi informatica ha delle conoscenze pregresse in ambito IT, sicuramente le sarà più semplice implementare gli steps.
Tuttavia, senza adeguate competenze di leadership e management, non sarà in grado di prendere le decisioni migliori.

Se hai una micro-impresa, sembra scontato che dovrai formarti a dovere e prendere accordi con collaboratori esterni di cui ti fidi.

Se hai una media impresa, è bene che deleghi tale responsabilità a una persona interna di fiducia.
Inoltre, ricordiamo che la risposta ad una crisi informatica può essere implementata anche da remoto!

Unità 2: Rispondere a una crisi informatica

Sezione 2.2: Il piano backup

In una PMI, il piano backup può differire a seconda del settore, e del tipo di business ecc..

Tuttavia, devi considerare I seguenti passaggi:

Conosci i tuoi fornitori

Mantieni al sicuro i contatti di tutti i tuoi fornitori. Dato che un attacco può essere attuato dalla tua rete locale, persino se non sei connesso ad Internet, le tue password e le informazioni sensibili possono essere rubate in ogni momento.

Cosa fare:

Previeni ogni possible attacco prima che si verifichi e custodisci le informazioni di contatto dei tuoi fornitore anche in **forma cartacea**.

Erasmus+

Unità 2: Rispondere ad una crisi informatica

Sezione 2.2: Il piano backup

Segui le traccie

Se noti azioni sospette:

- Sul tuo profile bancario, chiama la banca e blocca tutte le tue carte;
- Sul tuo cloud aziendale, contatta il fornitore (telefonicamente o per email).

Cosa fare:
Evita di utilizzare le app/ clouds che possono essere infette. Contatta direttamente il fornitore.

Stacca la spina!

A volte, è l'unico modo per scongiurare un attacco.

Cosa fare:
Se noti qualcosa di sospetto sui tuoi devices o su quelli dei dipendenti, stacca la spina.

Erasmus+

Unità 2: Rispondere ad una crisi informatica

Sezione 2.3: Protocollo comunicativo in caso di crisi informatica

Rispondere adeguatamente ad una crisi informatica significa, anche, elaborare un protocollo comunicativo.
Ricorda che in questi casi la cosa più importante sono le tempistiche.
Comunica l'accaduto agli stakeholders il prima possibile.
È fondamentale che lo vengano a sapere da TE, non dai giornali o i media.
Fai capire loro che state cercando di sistemare il problema e avete già preso delle precauzioni per minimizzare le conseguenze.

L'azienda deve essere pronta per questa fase prima che si verifichi, perciò prepara la lista degli stakeholders:

- Clienti (specailmente quando li hai nel database sabotato)
- Collaboratori, sponsor, investitori
- I fornitori
- Il vicinato (potrebbe succedere anche a loro)

Unità 2: Rispondere ad un crisi informatica

Sezione 2.3: Protocollo comunicativo in caso di crisi informatica

Un'altra buona prassi è postare una dichiarazione sui profili aziendali e sul sito. Ovviamente, puoi delegarlo a un dipendente.
Una volta postata, la dichiarazione deve essere aggiornata con frequenza per far capire agli stakeholders che state sistemando il problema.

RICORDA: La sopravvivenza dell'attività dipenderai da come saprai gestire l'attacco cyber

Come parlare in merito alla crisi?

- ✓ Parla sempre chiaramente.
- ✓ Cita I fatti, non dare opinioni.
- ✗ Evita reazioni emotive.
- ✓ Dai risposte precise alle domande.
- ✗ Non accusare nessuno e non chiedere scusa prima di sapere cosa è successo.

Unità 3: Ripristinare l’attività dopo la crisi

Sezione 3.1: Come tornare alla normalità dopo una crisi?

Dopo la crisi, a piccoli passi devono essere ripristinate tutte le attività

Entriamo nel vivo della terza fase: il recupero dopo il disastro.

Il recupero dopo una crisi è il processo che aiuta l’organizzazione a ripristinare le attività operative quotidiane

Tale processo implica:

- valutazione (dei rischi, delle cause e della gestione)
- ‘lezioni imparate’
- Pianificazione dei miglioramenti

Erasmus+

Unità 3: Ripristinare le attività dopo una crisi

Sezione 3.2: Fai delle valutazioni!

Il recupero inizia dopo la crisi. Per essere sicuri che ciò che è accaduto non si verifiche più, è importante fare delle valutazioni per sanare i gap che hanno portato all'attacco:

- Pianifica dei meeting per stimare i danni e fare delle analisi sull'accaduto. Cerca di capire quali sono state la cause. Se necessario, richiedi un support esterno.

- Valuta il tuo attuale piano di gestione in caso di crisi finanziaria. Analizzane tutte le fasi per capire cosa è andato storto.

Erasmus+

Unità 3: Ripristinare le attività dopo una crisi

Sezione 3.3: ‘Lezione imparata’

Dopo o durante l’analisi, fai una lista su tutte le possibili vulnerabilità che hanno reso più semplice realizzare l’attacco. Non vederla come una sconfitta, impara da ciò che è accaduto!

Se sei l’imprenditore, il tuo atteggiamento influenzerà quello dei tuoi dipendenti e dei tuoi stakeholders. Se consideri l’attacco come una sconfitta o accusi qualcuno ingiustamente, il futuro della tua attività potrebbe essere a rischio.

RICORDA: qualsiasi azione influenzerà non solo la situazione attuale ma anche la reputazione aziendale futura e i profitti!

Erasmus+

Unità 3: Ripristinare le attività dopo la crisi

Sezione 3.4: Pianifica i miglioramenti

L'ultimo step è quello di analizzare il gap attraverso i fatti e le informazioni.
Se dovessi scoprire che l'attacco è stato causato da una negligenza di un dipendente, evita reazioni troppo emotive. Ci sono differenti modi di reagire a seconda di quale sia stata la causa.
Sicuramente, la cosa migliore è pianificare dei miglioramenti di medio – e lungo- periodo per sanare i gap.
Ciascun gap ha potuto causare l'incidente. Ciascun obiettivo da raggiungere serve per evitare recidive in futuro.
Il processo di ripristino deve servire per eliminare o minimizzare il rischio che l'attacco si verifiche di nuovo.
Se questo non avviene, non hai imparato la lezione!

Unità 3: Ripristino delle attività dopo una crisi

Sezione 3.5: Caso studio – Marriot International

Non importa che tu abbia una piccola o una grande impresa, il rischio di essere hackerati esiste sempre. Di seguito, ti proponiamo due famosi case study a riguardo.

Marriott International

L'attacco informatico

La famosa catena di hotel, Marriot International, fu hackerata a Gennaio 2020, ma l'attacco non fu reso noto prima della fine di Febbraio. Gli hacker ottennero le credenziali di accesso al database clienti da due impiegati. L'azienda iniziò le investigazioni privatamente.

Erasmus+

Unit 3: Recovery after the cyber crisis

Sezione 3.5: Caso studio – Marriot International

Risposta

Marriot fece una dichiarazione in cui informo che degli hacker avevano avuto accesso ad informazioni personali come nome, data di nascita, lingua preferita e numero del profilo fedeltà.
Inoltre, inviò una mail a tutti gli ospiti implicati; creò una pagina web dedicata e un numero verde; informò i clienti di aver stipulato delle assicurazioni, incluso quella contro gli attacchi cyber.
La risposta è sembrata molto professionale e ,nella dichiarazione, Marriot ha affermato che i costi delle conseguenze non sono stati troppo significativi.

Ripristino delle attività

Ad Ottobre 2020, è stato imposto alla nota catena di hotel di pagare £18.4m per la violazione della privacy di 339 milioni di ospiti.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unità 3: Ripristinare le attività dopo la crisi

Sezione 3.5: Caso studio – Marriot International

Qual è la 'lezione imparata' ?

Prima di tutto, è da specificare che questo non fu il primo attacco informatico subito da Marriot International. Nel 2014, gli hackers presero di mira il gruppo Starwood Hotels, acquisito da Marriot due anni prima.

Da quello che sappiamo, l'azienda prese precauzioni e l'episodio si verificò di nuovo nel 2018. Anche in questo caso non fu seguito nessun protocollo, perciò gli hackers hanno continuato ad infettare i sistemi, incluso:

- nomi
- indirizzi email
- numeri di telefono
- numero del passaporto
- info su arrivi e partenze
- VIP
- numero del profile fedeltà

Unità 3: Ripristinare le attività dopo la crisi

Sezione 3.5: Caso studio – Marriot International

La nota catena di Hotel, quindi, non ha adeguatamente rispettato il Regolamento Generale per la Protezione dei Dati (GDPR), questo è il motivo per cui è stata multata.
Inoltre, l'errore si è ripetuto più di una volta, ciò significa che i responsabili per la gestione delle crisi informatiche non sono riusciti a sanare adeguatamente i gaps.

Cosa ha aiutato?

Il fatto che, alla fine, Marriot International si sia dotata di un'assicurazione contro questo tipo di danni.

What can you learn from this?

Unità 3: Ripristinare le attività dopo la crisi

Sezione 3.5: Caso studio – Marriot International

‘’Lezione imparata’:

- **Ridefinire come gestire una crisi informatica.**
- **Pensare se si hanno abbastanza abilità di leadership e management**
- **Sapere come implementare il piano di gestione di una crisi**
- **Se non è sufficiente, segui altri nostril corsi a riguardo.**
- **Fatti supportare da un professionista esterno.**
- **Valuta l’opzione di acquistare un’assicurazione.**

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unità 3: Ripristinare le attività dopo una crisi

Sezione 3.6: Sintesi

Oggi, saper gestire una crisi finanziaria è importante tanto per le PMI quanto per le GI.

La differenza sta nelle risorse a disposizione: più piccola è l'attività, maggiori saranno le responsabilità per l'imprenditore.

Ricorda: gli attacchi informatici possono verificarsi anche se il tuo business non è principalmente online.

Se possiedi un laptop, uno smartphone, una stampante, devi sapere come gestire questo tipo di problematica perché non farlo significherebbe ampliare la crisi o crearne una nuova!

Buona fortuna!

Erasmus+

Bibliografia e Sitografia

The New Statesman > **How to tell your customers you've been hacked**

https://www.newstatesman.com/spotlight/2019/09/how-tell-your-customers-you-ve-been-hacked

Deloitte > **Cyber crisis management: Readiness, response, and recovery**

https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf

Security Boulevard > **Marriott Data Breach 2020: 5.2 Million Guest Records Were Stolen**

https://securityboulevard.com/2020/04/marriott-data-breach-2020-5-2-million-guest-records-were-stolen/#:~:text=The%2520breach%2520was%2520identified%2520at,have%2520accessed%2520the%2520guest%2520details.

BBC News > **Marriott Hotels fined £18.4m for data breach that hit millions**

https://www.bbc.com/news/technology-54748843

Marriott International News Center > **Marriott International Notifies Guests of Property System Incident**

https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident

Forbes > **What Businesses Are The Most Vulnerable To Cyberattacks?**

https://www.forbes.com/sites/theyec/2021/01/19/what-businesses-are-the-most-vulnerable-to-cyberattacks/?sh=1c1c8f663534

Grazie per l’attenzione!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.