Esempi di sinistri

1 Un dipendente della scuola prepara una lista di studenti partecipanti ad una gita; nell'inviarla all'albergo e agli organizzatori della trasferta, accidentalmente allega un file non pertinente e contenente i dati personali relativi a tutti gli studenti e operatori della scuola con nominativi, indirizzi e documenti di identità.

Danni: costi di notifica; spese legali di difesa; risarcimento a favore di terzi.

Garanzie attivate: violazione degli obblighi di riservatezza; Incident Response team.

2 Una scuola ha affittato una fotocopiatrice per un periodo di due anni. La macchina ha immagazzinato numerose informazioni sensibili di studenti e dipendenti. Allo scadere del contratto d'affitto, la scuola restituisce la macchina alla società concedente e un dipendente di quest'ultima accede e utilizza i dati contenuti in essa per scopi infausti.

Danni: investigazioni di esperti di informatica forense; consulenza legale; servizi di call center; servizi di monitoraggio e ripristino dell'identità.

Garanzie attivate: perdita di dati; responsabilità derivante da violazione di obblighi di riservatezza.

3 Un dipendente di una scuola ha ignorato le policy interne in materia di sicurezza e ha aperto un file, apparentemente innocuo ma contenente un virus, allegato ad una e-mail. Il giorno successivo, il sistema informatico utilizzato per l'attività ordinaria della scuola non funziona, impedendo il regolare svolgimento delle attività.

Danni: investigazioni di esperti di informatica forense; ripristino dei sistemi; aumento dei costi del lavoro; fermo d'attività scolastica.

Garanzie attivate: perdita di dati; interruzione d'attività.

4 Un soggetto malintenzionato ha trafugato nome utente e password di un docente per accedere al registro elettronico e ha estrapolato dati sensibili degli studenti (anagrafica e voti scolastici).

Danni: costi di notifica; spese legali di difesa; risarcimento a favore di terzi.

Garanzie attivate: violazione degli obblighi di riservatezza.

CYBER *insurance*

La polizza che copre Dirigente Scolastico e Scuola dai danni e dalle spese derivanti dalle responsabilità per i rischi informatici

intermediato da

abz broker

CYBER INSURANCE è la polizza per i cyber rischi, creata in collaborazione con Abz Broker, in esclusiva per gli Istituti Scolastici clienti di **CLASSEVIVA** per coprire **tutti i danni e le spese derivanti da responsabilità dell'Istituzione Scolastica e del Dirigente Scolastico per i rischi informatici**

Aderendo da ora, sei assicurato da subito, ma paghi il premio solo per il 2021

Con il patrocinio di:
GRUPPOSPAGGIARIPARMA

La Scuola del futuro, oggi

CYBER *insurance*

Il rischio informatico, o Cyber Risk, **è l'insieme dei danni derivanti da azioni accidentali o intenzionali che riguardano software, dati e informazioni gestiti e conservati in formato digitale.**

La scuola negli ultimi anni ha vissuto un aumento dei rischi informatici, sia per la digitalizzazione del sistema scolastico stesso, sia per lo svolgimento della didattica online a causa della pandemia Covid-19, con diversi sistemi non sempre consoni o sicuri.

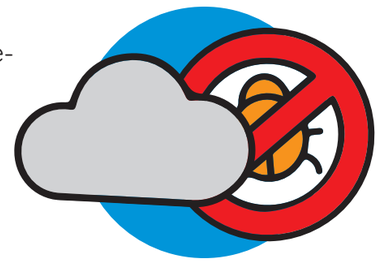
Inoltre, le attività didattiche, svolte attraverso piattaforme tecnologiche, e la necessità di collegamento con il M.I. per lo scambio di dati e informazioni fanno sì che le scuole siano sempre più immerse in un ecosistema digitale.

Il processo di digitalizzazione, fortemente accelerato dalla problematica derivante dal Coronavirus, **ha naturalmente aumentato l'esposizione delle scuole al rischio informatico: intrusioni e accessi non autorizzati con alterazione, furto e distruzione di dati, installazione di malware, phishing.**

Gli attacchi informatici a Istituti Scolastici sono in continua crescita: nel 2019 sono triplicati in numero e aumentati di gravità rispetto all'anno precedente.

Inoltre, l'entrata in vigore del GDPR (la normativa sulla protezione dei dati), **con sanzioni pesantissime per chi perde o diffonde dati senza autorizzazione,** e il Codice dell'Amministrazione Digitale (D.L. n. 82/2005) **aumentano le responsabilità delle Istituzioni Scolastiche.**

Ma quali sono i danni di un attacco informatico?



- **possono essere danni economici,** se la scuola deve sostenere dei costi per il recupero o il ripristino dei dati, o per l'interruzione delle attività;
- **possono essere legali,** se la scuola è chiamata in causa da persone che hanno subito danni (per esempio per violazione della privacy);
- **possono essere di immagine,** come la manipolazione del sito web o delle pagine social, o se la scuola deve sospendere temporaneamente la propria attività.

Quali sono gli strumenti per difendersi?

Oltre ad **aver scelto una piattaforma digitale sicura**, la scuola deve fare **formazione sui rischi informatici al personale e agli studenti.** Queste misure sono fondamentali, ma non eliminano del tutto il Cyber Risk. **La soluzione per risolvere il rischio residuo è la stipula di una polizza assicurativa che copra i danni derivanti da Cyber Risk.**

Il Cyber Risk non comprende soltanto gli incidenti causati da fattori esterni; un'ampia percentuale di sinistri è imputabile ai dipendenti e agli alunni. I principali fattori di rischio sono: scansioni di documenti cartacei, **errori umani, dipendenti infedeli, tentativi di hackeraggio** degli alunni, **perdita di dispositivi e uso "leggero" della password.**

Cosa offre Cyber Insurance alla scuola CLASSEVIVA

RESPONSABILITÀ CIVILE

La polizza rimborsa i danni e le spese legali derivanti da richieste di risarcimento relative a:

- **VIOLAZIONE OBBLIGHI DI RISERVATEZZA:** violazione di dati personali, di informazioni aziendali di terzi, la violazione involontaria delle norme sulla privacy.
- **VIOLAZIONE SICUREZZA DELLA RETE:** nel caso in cui i sistemi dell'assicurato siano utilizzati per condurre un attacco a terzi.
- **RESPONSABILITÀ DERIVANTE DAI MEDIA:** in caso di violazione del copyright nell'ambito dei contenuti multimediali pubblicati online o nei casi di diffamazione, oltraggio, plagio.

PERDITE DIRETTE

La polizza copre, inoltre, i costi sostenuti a seguito di:

- **CYBER ESTORSIONE:** rimborsa il riscatto e paga le spese a seguito di una cyber estorsione.
- **PERDITA DEI DATI:** copre i costi per il recupero e il ripristino dei dati.
- **INTERRUZIONE D'ATTIVITÀ:** copre le perdite e i maggiori costi sofferti.
- **SPESE EXTRA:** copre i costi i per rimuovere malware dal sistema informatico e per ricostruire i dati.
- **FONDO RICORSO CONSUMATORI:** per il deposito obbligatorio in caso di procedimento dell'Autorità di Vigilanza.
- **SPESE DI INCIDENT RESPONSE:** per una società di informatica forense, per ottemperare alle norme sulla privacy, per un consulente legale.