ASSITECA
CONSULTATIVE BROKER

ANCE TORINO
COLLEGIO COSTRUTTORI EDILI

ANCE PIEMONTE VALLE D'AOSTA

Implementazione del GDPR: aspetti operativi e sicurezza informatica per le imprese di costruzione.

Le nuove norme per la protezione dei dati per le imprese di costruzioni: adempimenti e responsabilità

giovedì 21 giugno 2018

ASSITECA
Chi siamo

L'unica realtà di servizi professionali creata per assistere le aziende nella **gestione integrata dei rischi d'impresa.**

- **Nata nel 1982**, oggi è il **primo gruppo italiano nel mercato del brokeraggio assicurativo**.
- Dal luglio 2015 è **quotata alla Borsa Italiana** – Segmento AIM Italia.
- Attività: **analisi dei rischi, consulenza, intermediazione e gestione del portafoglio assicurativo**.

CERTIFICAZIONI

- Bilancio civilistico e consolidato certificato dal 1985.
- Certificazione di Qualità secondo la norma ISO 9001:2008 dal 1997
- Bilancio Sociale dall'anno fiscale 2002/2003.
- Codice Etico e Modello Organizzativo ai sensi del D.Lgs. 231/01 in vigore dal 2004.

65 milioni di ricavi

20 sedi in Italia

100 rappresentanze nel mondo

577 dipendenti e collaboratori

3.975 aziende clienti

4.985 analisi di rischio effettuate

650 milioni di premi intermediati

LA NUOVA REGOLAMENTAZIONE IN PILLOLE

Informazioni generali

ASSITECA CONSULTATIVE BROKER

DRIVER E APPLICABILITÀ

- Cyber Risk:
- Digital Single Market
- Big Data e Cloud
- Riguarda tutte le organizzazioni pubbliche e private
- Si applica a tutti i residenti UE anche se i dati sono trattati fuori dall'UE o da imprese extra UE

OBBLIGHI

- DPO: la nomina di un Data Protection Officer è obbligatoria per le imprese che processano elevati volumi di dati e le PA e consigliabile per le altre
- DPIA: i processi con rischi elevati per i dati personali dovranno essere sottoposti ad una analisi di rischio
- Comunicazione di data breach; Privacy by Design; Privacy by Default; registro trattamenti; Cyber Security Policy; informative; nomine; formazione.

NUOVI DIRITTI e ATTENZIONE AI DATI PERSONALI

- Accesso; trasparenza (consenso, revoche, minori); cancellazione/oblio; portabilità; opposizione - sospensione
- Definizione più ampia che include anche: dati genetici, sulla salute fisica e mentale, biometrici, economici, identità sociale e culturale, giudiziari

ACCOUNTABILITY (responsabilità)

- I soggetti che trattano i dati hanno responsabilità più chiare e devono dimostrare come hanno tutelato i dati personali
- Certificazioni e codici di condotta possono aiutare a dimostrare la conformità

! ! !

SANZIONI PIU' DURE

Multe fino a 20 mln € oppure al 4% del fatturato di gruppo, se superiore

I COSTRUTTORI EDILI TRATTANO DATI PERSONALI?

ASSITECA
CONSULTATIVE BROKER

1. Gestione dei dati del personale
2. Gestione dei dati dei clienti e dei fornitori
3. Dati sulla formazione del personale
4. Dati sulla sicurezza sul lavoro
5. Dati relativi alla gestione informatica

DATI DEL PERSONALE

1. GESTIONE DEI DATI DEL PERSONALE							
TIPOLOGIA DATI	• Dati identificativi • Dati particolari						
TIPOLOGIA DEL TRATTAMENTO	• Amministrazione gestione del personale	• Assunzioni - collaborazioni - dimissioni licenziamenti - provvedimenti disciplinari	• Iscrizione a sindacati • Inserimento in Registri cartacei ed elettronici	• Rilevazione e normalizzazione delle presenze	• Valutazione del personale	• Pagamento stipendi/ emolumenti	• Verifica congruità pagamento delle note spesa
CATEGORIA DI INTERESSATI	• Dipendenti dell'impresa	• Professionisti non dipendenti (consulenti, periti, assicuratori, revisori fiscali)					
DESTINATARI DEI DATI	• Personale interno	• Istituzioni • Autorità di Vigilanza	• Soggetti terzi (gestione contabilità e buste paga)	• Autorità giudiziaria			
TEMPI DI CONSERVAZIONE	• 10 anni o specificare eventuali altri termini						
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Divulgazione non autorizzata	• Uso improprio			
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare tecnico	• accessi riservati al personale autorizzato	• protezione archivi informatici	• protezione fisica documenti	• backup • antivirus	• password	

DATI DI CLIENTI E FORNITORI

2. GESTIONE DEI DATI DEI CLIENTI E DEI FORNITORI				
TIPOLOGIA DATI	• Dati personali/ identificativi dei referenti di clienti e fornitori	• Immagini personali	• Dati personali/ identificativi di clienti e fornitori	• CV Clienti e fornitori
TIPOLOGIA DEL TRATTAMENTO	• Inserimento in registri	• Gestione rapporto commerciale (stipula contratti, invio corrispondenza)	• Utilizzo dati per fatturazione	
CATEGORIA DI INTERESSATI	• Clienti/Fornitori			
DESTINATARI DEI DATI	• Personale interno	• Autorità di Vigilanza		
TEMPI DI CONSERVAZIONE	• 10 anni			
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Divulgazione non autorizzata	• Uso improprio
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare tecnico			

DATI SULLA FORMAZIONE

3. DATI PERSONALI SULLA FORMAZIONE PROFESSIONALE DEL PERSONALE					
TIPOLOGIA DATI	• Dati personali/ identificativi	• Dati relativi al percorso professionale/ formativo	• Dati particolari (per esonero)	• Immagini personali anche tramite ripresa	
TIPOLOGIA DEL TRATTAMENTO	• Piani formativi	• Formazione • Formazione in materia di D.Lgs n. 231/2001	• Erogazione corsi formazione interna	• Gestione eventi formazione	• Relazione con soggetti terzi
CATEGORIA DI INTERESSATI	• Personale dipendente	• Soggetti terzi (professionisti coinvolti negli eventi formativi)			
DESTINATARI DEI DATI	• Personale Interno	• Soggetti terzi certificatori • Autorità di Vigilanza			
TEMPI DI CONSERVAZIONE	• Non determinato				
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Divulgazione non autorizzata	• Uso improprio	
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare Tecnico				

DATI SULLA SICUREZZA SUL LAVORO

4. DATI PERSONALI SULLA SICUREZZA SUL LAVORO (D.LGS. N. 81/2008 E S.M.)					
TIPOLOGIA DATI	• Dati personali/ identificativi	• Immagini personali anche tramite riprese	• Dati particolari	• Dati biometrici relativi alla salute (visibili solo da Rls e dal medico competente)	
TIPOLOGIA DEL TRATTAMENTO	• Visite mediche periodiche del personale	• Formazione del personale	• Adempimenti di cui al D.L.gs n. 81/2008	• Verifica dell'idoneità tecnico professionale dei dipendenti	
CATEGORIA DI INTERESSATI	• Personale dipendente				
DESTINATARI DEI DATI	• Medico competente	• Soggetti terzi certificatori	• Autorità di Vigilanza (Asl, Ispettorato lavoro, vigili del fuoco ecc.)	• Ente certificatore privato per la sicurezza	• RLS/RLST
TEMPI DI CONSERVAZIONE	• Non determinati				
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Divulgazione non autorizzata	• Uso improprio	
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare Tecnico				

SISTEMI INFORMATIVI?

5. DATI RELATIVI ALLA GESTIONE INFORMATICA				
TIPOLOGIA DATI	• Dati personali/ identificativi	• Dati particolari		
TIPOLOGIA DEL TRATTAMENTO	• Gestione autorizzazione di accesso al sistema informatico	• Gestione attività per sicurezza, integrità e disponibilità dei dati trattati con mezzi automatizzati		
CATEGORIA DI INTERESSATI	• Personale dipendente	• Soggetti terzi (fornitori, operai iscritti alla Cassa, consulenti esterni)		
DESTINATARI DEI DATI	• Personale Interno	• Soggetti esterni che collaborano per la gestione del sistema informatico		
TEMPI DI CONSERVAZIONE	• 10 anni			
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Accesso non autorizzato al sistema informatico	• Uso improprio
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare Tecnico			

DATI SULLA QUALITA'

6. CONTROLLI DI QUALITÀ					
TIPOLOGIA DATI	• Dati personali/ identificativi				
TIPOLOGIA DEL TRATTAMENTO	• Acquisizione dati previsti e indicati dallo standard internazionale sulla qualità (UNI EN ISO)	• Dati dipendenti e soggetti terzi impiegati nelle verifiche di conformità alle procedure per la formazione	• Comunicazione al Responsabile Qualità		
CATEGORIA DI INTERESSATI	• Personale dipendente	• Soggetti terzi (appalto, cooperativa esterna)	• Fornitori		
DESTINATARI DEI DATI	• Personale Interno	• Autorità di Vigilanza	• Clienti		
TEMPI DI CONSERVAZIONE	• 10 anni				
RISCHI SPECIFICI INERENTI I DATI	• Perdita	• Distruzione	• Divulgazione non autorizzata	• Uso improprio	• Rischio specifico: divulgazione dati in grado di rilevare inadempienze
MISURE DI SICUREZZA E TIPO DI PROCESSI A CUI I DATI SONO SOTTOPOSTI	• Disciplinare Tecnico				

COME MUOVERSI

Misure tecniche e organizzative

COMPLIANCE

- Aggiornare il modello organizzativo in tema di privacy, in ottemperanza alle responsabilità derivanti dal nuovo regolamento
- Creare un registro dei trattamenti di dati personali
- Definire o rivedere l'impianto documentale, in termini di policy, procedure, incarichi e deleghe, per il rispetto dei requisiti di accountability, anche per dimostrare la conformità
- Definire contrattualmente il rapporto tra Titolare e Responsabile del trattamento dati
- Rivedere Informative sulla Privacy; moduli e procedure per la raccolta dei consensi (anche on-line) per garantire la trasparenza verso i clienti
- Definire procedure di controllo e reportistica per garantire la conformità nel tempo

ORGANIZZAZIONE

- Rivedere e aggiornare i processi per la gestione del consenso e le modalità di interazione con gli interessati (oblio, accesso ai dati, portabilità dei dati, revoca, opposizione)
- Aggiornare il modello organizzativo per la nomina del DPO (Data Protection Officer)
- Definire un piano adeguato di formazione e informazione verso i dipendenti
- Descrivere i processi di trattamento dei dati e flussi degli stessi verso le terze parti
- Applicare il concetto di Risk Management ai processi di trattamento dei dati (DPIA – Data Protection Impact Assessment) e integrare con Information Security

COME MUOVERSI

Misure Information Technology

INFORMATION SECURITY

- Identificare e classificare i dati personali all'interno dell'azienda e definire i controlli da applicare in base alla classificazione
- Definire ed implementare le misure di sicurezza adeguate per la protezione dei dati personali
- Definire ed implementare le misure tecniche per pseudonimizzazione, anonimizzazione e/o cifratura dei dati
- Definire la metodologia e le misure per garantire la protezione dei dati fin dalla fase di progettazione (Privacy By Design), senza eccesso di trattamento (Privacy by Default)
- Supportare l'esecuzione della valutazione dei possibili impatti, attraverso la Data Protection Impact Analysis (DPIA), per i trattamenti definiti ad alto rischio
- Rivedere e/o implementare la procedura per data breach detection e data breach notification

INFORMATION TECHNOLOGY

- Supportare la mappatura dei dati personali sui sistemi informativi interni ed i flussi verso i sistemi esterni
- Implementare procedure per la gestione e cancellazione dei dati sui software che trattano dati personali
- Disegnare ed implementare delle procedure informatiche per rispondere alle richieste degli interessati (ad es. richiesta di portabilità, accesso ai dati, raccolta e revoca consensi, cancellazione)
- Sviluppare procedure IT per il tracciamento dei consensi e delle richieste degli interessati
- Applicare ove possibile la cifratura dei dati
- Implementare procedure di data backup e disaster recovery per rendere sempre fruibili i dati agli interessati

APPROCCIO METODOLOGICO

INTERVENTI SPECIFICI

- Registro trattamenti
- DPIA
- Piano di Emergenza
- Cyber Security Policy
- DPO
- Formazione

1 ANALISI E PROGETTAZIONE
- Risk Assessment
- Definizione obiettivi riduzione rischi

2 IMPLEMENTAZIONE
- Adeguamenti formali e documentali
- Interventi organizzativi
- Cyber Security

3 MONITORAGGIO E CONTROLLO
- Aggiornamenti
- Audit annuali

4 TRASFERIMENTO RISCHIO RESIDUO
- Polizze Rischi Cyber

LA METODOLOGIA ASSITECA

Fasi di intervento

1. ANALISI E PROGETTAZIONE

1. **Analisi documentale e organizzativa:**
   - Aspetti legali
   - Struttura interna
   - Information Technology
2. **Gap analysis**
3. **Progettazione** interventi
4. Definizione del **Piano di adeguamento**

2. ADEGUAMENTO

Area Documentale

- Rielaborazione moduli informativa Privacy
- Verifica procedure raccolta consensi al trattamento e aggiornamento modulistica on line e off line
- Verifica tutela diritti interessati
- Verifica applicazione dei concetti di Privacy By Default.
- Revisione nomine e deleghe interne e esterne
- Individuazione di eventuali corresponsabili
- Predisposizione/aggiornamento dell'organigramma privacy
- Ricostruzione processi e flussi dei dati personali
- Nomina DPO

Area Organizzativa

- Ricostruzione processi e flussi dei dati personali
- Formazione personale su Cyber Security e GDPR
- Formazione responsabili IT sui concetti di Privacy by Design e by Default
- Predisposizione Cyber Security Policy e Codice Disciplinare
- Predisposizione Registro Trattamento Dati
- Predisposizione Piano di Emergenza Cyber e procedura Comunicazioni Data Breach (violazioni)
- DPO (se necessario)
- Predisposizione DPIA – Data Protection Impact Analysis (se necessaria)

Area IT

- FASE 1 – Information security review e predisposizione adempimenti formali
  - Assessment dell'organizzazione e delle procedure IT in ambito cyber security
  - Definizione misure tecniche minime di protezione dati personali.
  - Elaborazione dei contenuti tecnici per i documenti legali (es. registro trattamento dati; cyber security policy; DPIA; piano di emergenza data breach).
  - Verifica trasferimento di dati in paesi terzi.
  - Verifica procedura di backup IT.
- FASE 2 – Verifica vulnerabilità esterne (WAPT web e VA-PT reti wifi)
- FASE 3 – Verifica vulnerabilità interne (VA-PT LA e host - server . Client –netwrork device)
- FASE 4 – Verifica vulnerabilità applicativi aziendali (VA-PT applicativi)

3. MONITORAGGIO

Area Documentale

- Aggiornamento documentazione
- Analisi evoluzione normativa (comunicazioni Authority)
- Audit annuale

Area Organizzativa

- DPO Esterno
- Supporto al DPO interno
- Formazione GDPR e CYBER continuativa
- Aggiornamento DPIA

Area IT

- Vulnerability Assessment e Penetration Test
- Formazione specialistica:
  - ✓ Sicurezza logica (responsabili)
  - ✓ Policy aziendali (dipendenti)
- Checkup Sistemi Informativi

CYBER SECURITY: LO SCENARIO È CAMBIATO

Dalla guerra fredda a quella cyber

NUOVE FORME DI DELINQUENZA

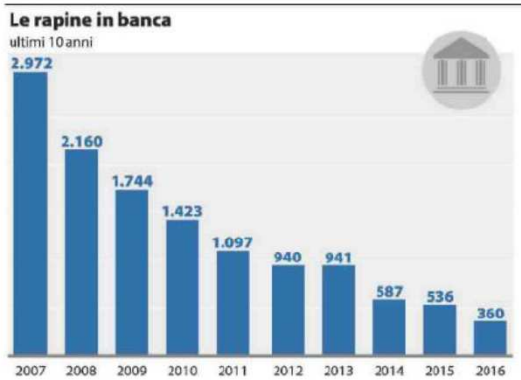
del 08 Maggio 2017

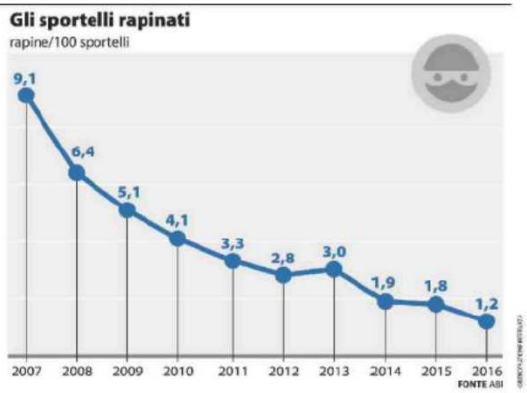
la Repubblica
QUOTIDIANO: ROMA

estratto da pag. 20

Il risparmio

Dopo anni di calo, nel 2016 un nuovo crollo: solo 360 casi, ma crescono le truffe informatiche





Rapine in banca in via d'estinzione anche per i ladri il bottino è digitale

ROSARIA AMATO

la grande distribuzione, pompe di benzina, locali. «Ma in

ti spesi circa 600-700 milioni di euro tra misure di sicurez-

NUOVE FORME DI DELINQUENZA

STUDIO ACCENTURE SU 254 GRANDI IMPRESE

I cyber-attacchi costano alle aziende 11,7 milioni di dollari all'anno (in media)

–di L.Tre | 26 settembre 2017

NUOVE FORME DI DELINQUENZA

Hackers shut down plant by
targeting its safety system
It's the first known attack of its kind.

jon Fingas, 12.17.17
Hackers have already attacked critical infrastructure, but now they're launching campaigns that could have dire consequences. FireEye reported that a plant of an unmentioned nature and location (other firms believe it's in the Middle East) was forced to shut down after a hack targeted its industrial safety system -- it's the first known instance of a breach like this taking place. While the digital assault was clearly serious in and of itself, there are hints that it could have been much worse.
The malware, nicknamed Triton, hijacked a workstation using Schneider Electric's Triconex safety technology (typically used in power plants). The culprits hoped to modify controllers that could pinpoint safety problems, but some of those controllers entered a failsafe state in response and shut down the plant, leading operators to conduct the investigation that caught the hostile code. Triton was otherwise fairly sophisticated. It would try to recover failed controllers to avoid raising alerts, and would even overwrite its own programs with junk data if it couldn't salvage a controller inside of a given time window.
The hack wasn't made possible by a flaw in Triconex itself, FireEye noted. Instead, it appeared to be an "isolated incident."
While it's not certain who's responsible, FireEye said the hack was "consistent" with a "nation state" readying an attack. And that's concerning, especially if the perpetrators learn from their mistakes. While shutting down a power plant would be bad enough, it'd be worse if the malware could fool a safety system into allowing attacks that would damage the facility and lead to a long-term shutdown or an environmental disaster. In short, companies and governments alike may have no choice but to prioritize defending critical infrastructure if they want to avoid crippling attacks.

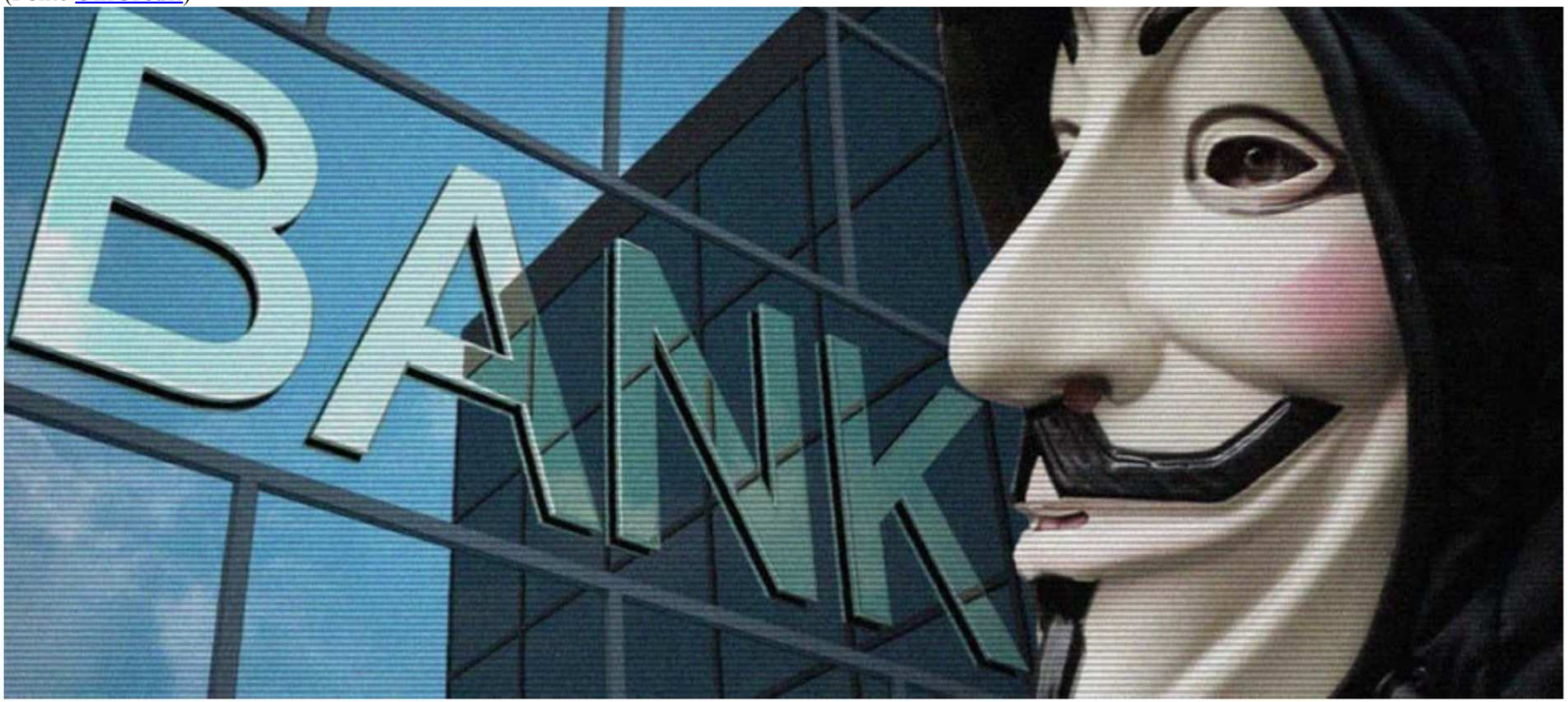
NUOVE FORME DI DELINQUENZA

UNICREDIT: ATTACCO HACKER
VIOLATI I DATI DI 400.000 CLIENTI

UniCredit sotto attacco, violati i dati di 400.000 clienti

Unicredit ha subito due consistenti attacchi informatici, con sottrazione dei dati anagrafici di circa 400.000 clienti.

di
*Alessandro Crea*Tom's HardwareRedattore
26 Luglio 2017, 10:30
(Fonte **UniCredit**)



NUOVE FORME DI DELINQUENZA

Deloitte, email al soldo dei cyber criminali

Un'altra grande azienda è finita nel mirino dei cyber-criminali. Questa volta il data breach riguarda la società di consulenza Deloitte, eletta solo qualche anno fa come migliore azienda in tema di cyber sicurezza

Roma - **Un attacco hacker ha aperto una breccia nei database di Deloitte**, azienda di consulenza e revisione, prima al mondo in termini di ricavi e numero di professionisti. L'attacco è venuto alla luce solo ora, nonostante sia perdurato per mesi a partire da ottobre/novembre 2016. Deloitte se ne sarebbe accorta solo a marzo avviando un'indagine interna. I cyber-criminali avrebbero ottenuto accesso privilegiato al server di posta, **intromettendosi nelle comunicazioni elettroniche tra l'azienda e i suoi clienti**. Favoriti dall'assenza di un sistema di autenticazione a due fattori, sono riusciti ad ottenere informazioni sensibili di numerosi clienti Deloitte, tra i quali spiccano grandi banche, multinazionali (anche farmaceutiche) e agenzie governative, come riportato da The Guardian.

NUOVE FORME DI DELINQUENZA

R.it | Cronaca

Mr. Confindustria a Bruxelles truffato da un hacker: persi 500mila euro. Licenziato

"Sposta subito mezzo milione su questo conto estero". Ma la mail era di un hacker. E i soldi sono spariti. Il finto ordine a firma della direttrice Panucci: "Esegui e non mi chiamare che sto fuori col presidente"

di ROBERTO MANIA

30 settembre 2017

Gianfranco Dell'Alba

ROMA - Ci sono circa cinquecentomila euro che da un conto della Confindustria sono finiti in un conto estero di cui ancora non si conosce l'intestatario. Soldi evaporati, per ora. C'è una mail falsa da cui è cominciato tutto. C'è un dirigente dell'associazione degli industriali licenziato in tronco per un bonifico che non avrebbe dovuto fare. È successo in Confindustria ma sono centinaia le aziende colpite ogni giorno da frodi finanziarie e milioni le mail contraffatte (mail spoofing, le chiamano gli esperti del settore) da cui partono ordini per spostare denaro in ogni parte del mondo.

NUOVE FORME DI DELINQUENZA

Virus informatico mette ko l'ufficio tecnico di Arco

Gio, 27/07/2017 - 05:57

28 CONNECT | TWITTER | 0 LINKEDIN | EMAIL | STAMPA

PER APPROFONDIRE:
comune, arco, virus, computer

Tempo di lettura: ! minuto 36 secondi

Un attacco informatico o piuttosto un virus elettronico ha messo a dura prova nei giorni scorsi l'ufficio tecnico del municipio di Arco, in modo particolare il disservizio riguarda circa quattrocento pratiche edilizie che risultano danneggiate dal fenomeno. Adesso è necessario rimboccarsi le maniche e rimettere a posto tutto il materiale disastrato con ordine e una pazienza infinita.

NUOVE FORME DI DELINQUENZA

Hacker sequestrano i server di un ospedale. Vogliono un riscatto in Bitcoin

L'attacco ha paralizzato
l'intera rete informatica.

Le informazioni sanitarie conservate nei sistemi informatici degli ospedali non sono preziose soltanto per il personale medico: la loro natura di "dati sensibili" fa sì che siano anche ghiotte prede per gli hacker. L'articolo continua qui sotto.

Lo scorso 11 gennaio si è avuta la dimostrazione di tutto ciò: in quel giorno l'Hancock Regional Hospital di Greenfield, Indiana (Usa) è rimasto vittima di un cyberattacco che ha compromesso l'intera rete informatica ospedaliera.

I computer si sono bloccati e hanno preso a mostrare soltanto una schermata che chiedeva il pagamento di un riscatto in Bitcoin: soltanto cedendo al ricatto - spiegavano gli autori dell'attacco - il personale dell'ospedale avrebbe potuto avere nuovamente accesso ai dati.

L'amministrazione ospedaliera non s'è però lasciata intimorire e ha deciso di spegnere ogni Pc, al fine di evitare il diffondersi di qualsiasi malware avesse colpito i computer, per poi contattare l'Fbi.

Le informazioni divulgate dagli investigatori sono a questo punto molto scarse, ma pare che l'attacco non sia stato facilitato da qualche tipo di errore umano, come un dipendente che abbocca a una email di phishing.

Attualmente la rete informatica dell'ospedale americano è tornata alla pieno operatività, ma l'Fbi non ha spiegato se il ritorno alla normalità sia stato ottenuto cedendo al ricatto oppure liberando il sistema dall'infezione. In ogni caso, l'amministratore della struttura ritiene che non ci sia stato alcun furto di dati.

Ciò di cui gli agenti federali statunitensi sono sicuri è che, a giudicare da quanto era sofisticato l'attacco, l'autore non era «un ragazzino quindicenne che vive nel seminterrato dei suoi».

In altre parole, non si è trattato soltanto di una ragazzata, ma dell'atto di un criminale con un obiettivo preciso.

NUOVE FORME DI DELINQUENZA

R.it | Sicurezza

DoubleLocker, il ransomware per Android che ruba i dati bancari

Il malware scoperto dai ricercatori di Eset: il virus cambia il Pin del dispositivo chiedendo un riscatto. E potrebbe evolversi in trojan bancario

di SIMONE COSIMI

14 ottobre 201

NUOVE FORME DI DELINQUENZA

ASSITECA
CONSULTATIVE BROKER

Bologna, Bruno Barbieri truffato online: "Tutta colpa del wi-fi"

Arrestata una 33enne nigeriana. Aveva violato l'home banking dello chef e chiesto dei bonifici urgenti via e-mail

di MATTEO RADOGNA

Pubblicato il 20 luglio 2017
Ultimo aggiornamento: 19 luglio 2017 ore 23:06

Lo chef Bruno Barbieri

I RISCHI

- **Le aziende tecnologicamente più avanzate, condizione imprescindibile per mantenersi competitivi nel mercato globale, sono gli obiettivi maggiormente attaccabili.**
- **Internet, social network e home banking vengono usati in modo sempre più diffuso sia in ambito privato sia in ambito lavorativo.**

La **poca consapevolezza** della **propria vulnerabilità** da parte dell'utente è ovviamente uno degli aspetti più sfruttati dal cyber crime e ne determina la facilità di realizzazione.

LE CONTROMISURE

Conoscere la minaccia aiuta senza dubbio a mettere in atto semplici azioni che possono impedire di cadere vittima dei più comuni rischi e fare la differenza.

È importante sottolineare che l'aggiornamento costante è fondamentale perché questi strumenti si evolvono ad una velocità esponenziale.

TIPI DI AGGRESSORI

- Crimine organizzato
- Insider
- Spie industriali
- Hacktivist
- Wannabe lamer, script kiddie

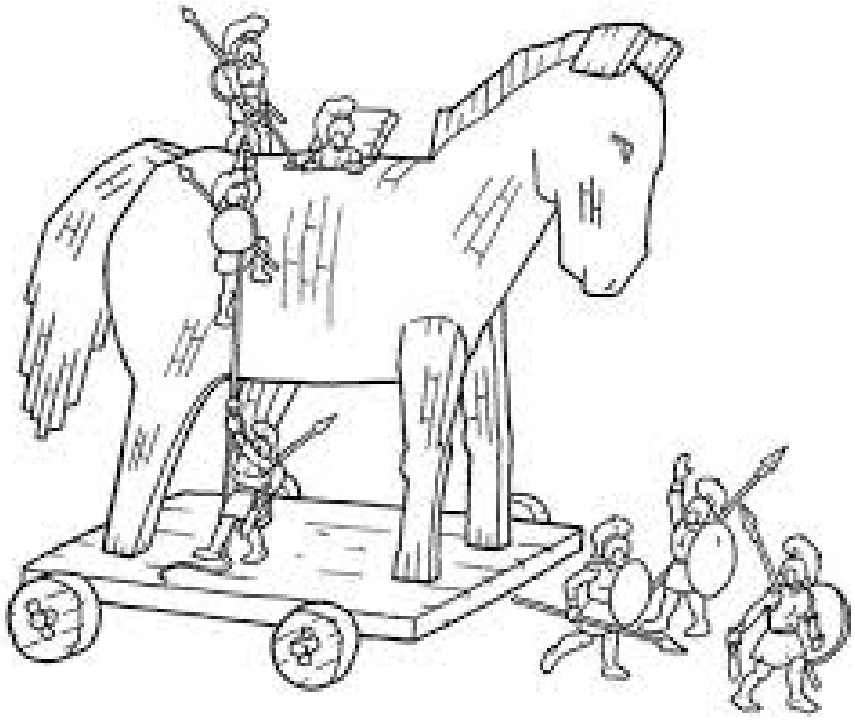
TIPI DI MINACCE

- Frodi
- Furto d'identità
- Furto di dati sensibili e di proprietà intellettuale
- Spionaggio
- Sabotaggio
- Attacchi dimostrativi
- Estorsione/Pizzo elettronico

VULNERABILITÀ UMANE

La prima breccia nella sicurezza di un sistema si ottiene non con strumenti tecnici, ma semplicemente sfruttando aspetti del comportamento umano:

- distrazione
- superficialità
- negligenza
- altruismo
- fiducia
- curiosità
- ignoranza



CONSIDERAZIONI

- **Difendersi dalle minacce in ambito cyber offre alle imprese un vantaggio competitivo.**
- **Il risk management aziendale è poco maturo nella gestione del rischio in ambito informatico.**

GESTIONE CYBER RISK: IL PERCORSO VIRTUOSO

PREVENZIONE

Strumenti di Prevenzione

=

Mirano a impedire il verificarsi dell'evento

o

Ritardarne l'accadimento

Information Security Review

Vulnerability Assessment

Penetration Test

Formazione

PROTEZIONE

Strumenti di Protezione

=

Consentono di minimizzarne gli effetti del danno

Sistemi di Protezione Fisica

Incendio / Allagamento

Separazione Supporti-Data Base

Back-Up Cloud

Disaster Recovery IT

Crisis Management Support

TRASFERIMENTO

Ritenzione del rischio in proprio

Trasferimento del rischio attraverso l'assicurazione per sottrarre l'impresa alle conseguenze finanziarie derivanti dal danno

TRASFERIMENTO:
LE NUOVE ASSICURAZIONI CYBER

ASSITECA CONSULTATIVE BROKER

Responsabilità Civile

Privacy Liability
- Violazione di dati personali
- Violazione di informazioni riservate (di terzi)
- Violazione involontaria delle Norme sulla privacy

Network Security Liability
- Violazione della sicurezza della rete aziendale

Media Liability
- Diffamazione, oltraggio, plagio
- Violazione di copyright nell'ambito della prestazione di servizi multimediali

Danni Coperti
Risarcimento; Spese legali; Computer Forensic
Spese di notifica; Spese di consulenza; Spese per PR

Danni propri

Business Interruption
La Compagnia pagherà le **perdite per interruzione delle attività** subite durante il **periodo di indennizzo** e i **costi di recupero**

Data Asset Loss
La Compagnia pagherà i **Costi di recupero** in conseguenza di un **incidente relativo a Data Asset Loss**

Cyber Extortion
La Compagnia pagherà il **riscatto** (ove non vietato dalla legge) e le **spese** a seguito di una ***cyber* estorsione**

Danni Coperti
Costi di decontaminazione; Costi di ricostruzione dei dati; Computer Forensic; Perdita di profitto; Spese di Consulenza; Incident Response

Estensioni

Incident Response
Gestione e pronto intervento in caso di crisi/disastro: Numero verde internazionale attivo 24/7; Discovery Plan; Computer Forensic; Consulenza tecnico/giuridica

Hardware
Danno ai dispositivi ubicati presso il locali dell'Assicurato o in viaggio (es: Centro Elaborazione Dati, dispositivi endpoint, dispositivi di archiviazione, etc…) utilizzati per archiviare, processare, modificare o controllare dati

Computer Crime
Perdita finanziaria a seguito del furto di denaro o titoli per mezzo di un attacco informatico perpetrato da parte di terzi.

Emanuele Capra

GDPR, Cyber Security e Business Continuity

emanuele.capra@assiteca.it

ASSITECA Consulting

www.assiteca.it