Evento di

Associazione Italiana Tesorieri d'Impresa

Main sponsor

INTESA SANPAOLO

IMI CORPORATE & INVESTMENT BANKING

Con il patrocinio

CONFINDUSTRIA EMILIA
AREA CENTRO: le imprese di Bologna, Ferrara e Modena

Partner didattico

Academy ask

20 novembre 2020 | ore 10.00

FRODE E CYBER RISK

Le frodi nei trasferimenti di denaro ha causato perdite per oltre $26 miliardi. Quali azioni per proteggere la tua azienda

Gianfilippo Pandolfini

Chief Operating Officer – BNL BNPParibas

Treasury Finance FORUM DAY 20 novembre 2020

Evento di

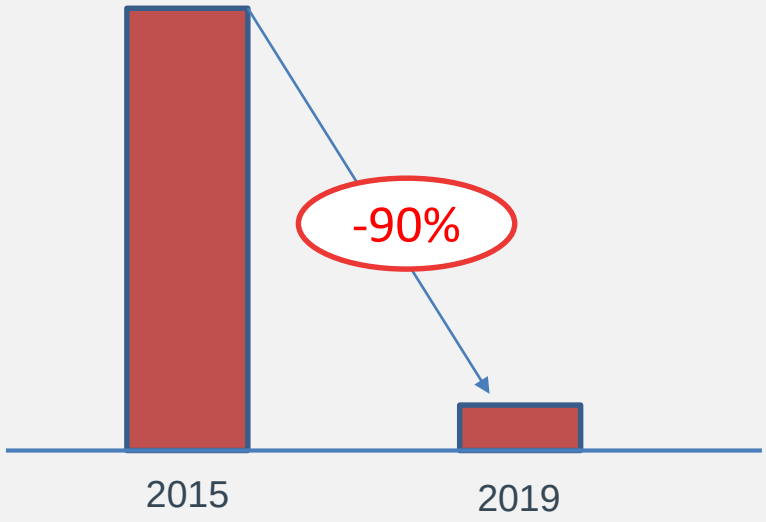
Main sponsor

Con il patrocinio

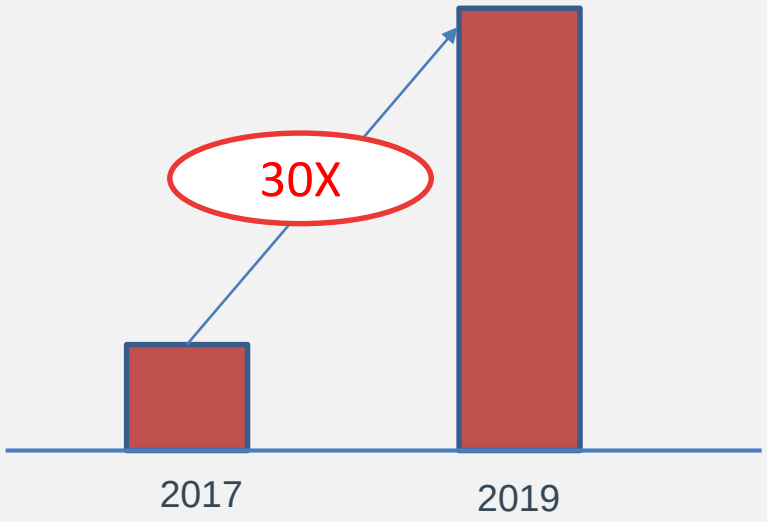
Partner didattico

LA POSTA IN GIOCO: UN FENOMENO IN CRESCITA

Numero rapine in Agenzia



Aziende Corporate che hanno subito furto delle credenziali



PRINCIPALI TIPI DI FRODE SUI PAGAMENTI

MALWARE

permette di impadronirsi del controllo della postazione di lavoro e modificare dati essenziali delle transazioni (codici IBAN di accredito, IBAN etc.).

PHISHING

Mail, sms, telefonate per carpire credenziali di autenticazione >> apparentemente provengono dalle banche e richiedono di inserire i codici di autenticazione su siti/applicazioni fake

SOCIAL ENGINEERING

I contatti avvengono per mezzo di canali tradizionali (e.g. telefono) e le transazioni vengono eseguite direttamente dalle vittime

Man in the Middle | **Ramsonware** | **DDOS** | **….**

ALTRE TIPOLOGIE DI CYBER RISK

FURTO - PERDITA DATI

l'utilizzo non controllato di USB, mail e navigazione Internet può comportare la fuoriscita / furto / perdita di informazioni riservate

INDISPONIBILITA' DEI SISTEMI

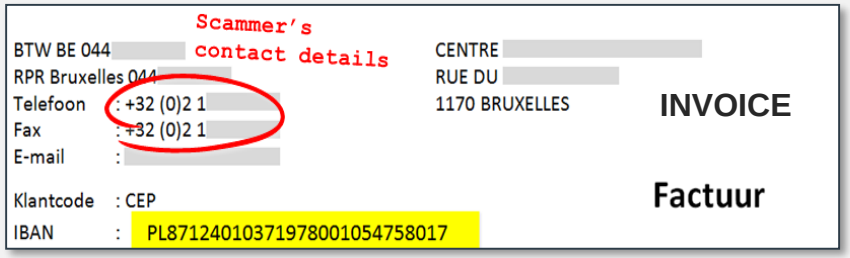
Malware / ransomware possono rendere indisponibili i sistemi informatici o essere vettori utilizzati per furto di dati

CONTINUITA' OPERATIVA

assenza di meccanismi di resilienza in grado di assicurare la continuità operativa in caso di guasti degli apparati o dei servizi collaterali

ALCUNI CASI REALI: LA TRUFFA DEL FINTO FORNITORE

Un Finto Fornitore ti informa (per email, posta o telefono) che il suo numero di conto bancario è cambiato e tutte le fatture devono essere pagate sul nuovo conto



SEGNALI DI ALLARME

- **Qualsiasi richiesta di modifica di un conto beneficiario** (attraverso posta, email, sulla fattura, o tramite telefono) o **aggiornamento dei contatti** di un fornitore (email, numero di telefono…)

PROTEGGITI

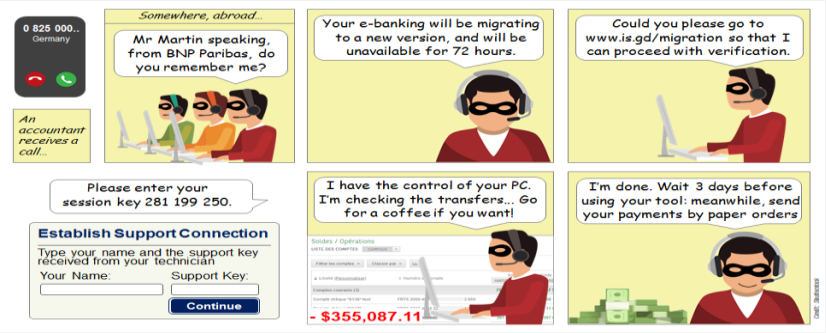
- **Verifica l'identità** del tuo contatto **utilizzando i tuoi soliti contatti** (e non quelli inviati tramite fattura)
- Presta particolarmente attenzione **ai tuoi principali fornitori**
- Sii particolarmente sospettoso **se il nuovo conto è domiciliato all'estero**
- **Autorizza poche persone a modificare i dettagli del fornitore** e introduci un doppio controllo

E RICORDA CHE I TRUFFATORI …

- … utilizzano lettere ufficiali **(**i truffatori generalmente rubano fatture reali dal fornitore)
- …. possono utilizzare indirizzi email simili a quelli del tuo fornitore, <u>se non del tutto uguali</u>

ALCUNI CASI REALI: LA TRUFFA DEL FINTO TECNICO

Sei contattato da un falso tecnico (dalla tua banca o dal fornitore di software), che vuole aiutarti ad implementare lo strumento bancario , eseguire un test, riemettere un bonifico, ecc.



SEGNALI DI ALLARME

- **Qualcuno si offre di aiutarti con gli strumenti di pagamento** quando non lo hai chiesto
- **Ti fa domande in merito agli strumenti di pagamento o procedure**
- **Ti chiede di collegarti ad un link che non conosci**, di **prendere il controllo del tuo PC da remoto**

PROTEGGITI

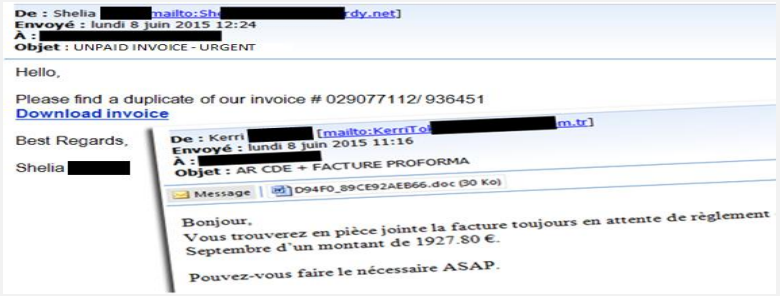
- **Non ti fidare dell'ID chiamante** (i truffatori possono impersonare il numero di telefono del tuo gestore)
- **Rifiuta di consentire a chiunque di prendere il controllo in remoto del tuo PC**
- **Non effettuare mai un test su richiesta del tecnico**

E RICORDA CHE I TRUFFATORI …

- … possono conoscere il nome del tuo gestore e le problematiche dei sistemi di pagamento
- … possono effettuare diverse chiamate preliminari per stabilire la fiducia ed ingannarti

ALCUNI CASI REALI: INFEZIONE DA SOFTWARE DANNOSI

Un dipendente ha aperto un allegato di una mail, dopo poco tempo i sistemi operativi dell'azienda smettono di funzionare e il mngt riceve una mail di richiesta di denaro



De : Shelia [mailto:Sh[redacted]rdy.net]
Envoyé : lundi 8 juin 2015 12:24
À : [redacted]
Objet : UNPAID INVOICE - URGENT

Hello,

Please find a duplicate of our invoice # 029077112/ 936451
Download invoice

Best Regards,

Shelia [redacted]

De : Kerri [redacted] [mailto:KerriTo[redacted]m.tr]
Envoyé : lundi 8 juin 2015 11:16
À : [redacted]
Objet : AR CDE + FACTURE PROFORMA

Message | D94F0_89CE92AEB66.doc (30 Ko)

Bonjour,
Vous trouverez en pièce jointe la facture toujours en attente de règlement Septembre d'un montant de 1927.80 €.

Pouvez-vous faire le nécessaire ASAP.

SEGNALI DI ALLARME

- **Qualsiasi email ricevuta da un contatto sconosciuto** contenente un link o un allegato
- Qualsiasi e-mail con un **oggetto insolito o contenuti intriganti**
- Qualsiasi file inviato via e-mail o scaricato, **contenente macro**

PROTEGGITI

- **Alla ricezione di un'email esterna verifica sempre il** mittente (è il suo solito indirizzo?)
- **Se apri un allegato f**allo su una workstation protetta da antivirus (non dallo smartphone), se hai dubbi non consentire l'esecuzione di macro
- Aggiorna il tuo sistema operativo e antivirus, blocca la chiavette USB e i siti di condivisione file

E RICORDA CHE I TRUFFATORI …

- …. spesso usano l'inoltro di link su DropBox, Google Drive, ...

LO SMARTWORKING E I RISCHI CYBER

…altera in qualche modo i principi di segregazione dei ruoli già in essere?

…. altera il rispetto dei principi di minimo privilegio già in essere?

…. viene alterato o ridurre il livello di efficacia dei controlli e dei processi precedentemente in essere?
(ad es. processi di controllo basati sull'esistenza di materialità (stampe etc.) non disponibili nel remote working)

…permette di rispettare le fasce orarie, i cut off e i presidi che venivano garanti e vincolati in virtu' della presenza fisica?

…sono in grado di controllare che nessuna attività o dato critico si svolga/transiti al di fuori di perimetri autorizzati e noti?

COME DIFENDERCI: UN GIUSTO MIX DI SOLUZIONI

Tecnologie

- Strumenti di **autenticazione / Profilazione**
- Patching
- Opportuna **segregazione delle risorse informatiche** sulle reti di trasmissione (e.g. utilizzo firewall)
- **Vulnerability assessment** continui / esercizi di red team
- **Antivirus/Antimalware**
- **…..**

+

Organizzazione

- C**ontrolli nel processo / segregazione dei ruoli**
- Analisi periodiche di **accessi anomali dei dipendenti** (es. ha fatto operazioni ma risultava in ferie; accessi ripetuti in un breve arco di tempo, etc.)
- **Security Operation Center e Cabina di regia** trasversale IT / Sicurezza / HR / Funzioni aziendali
- Esercizi di **Crisis management**
- Verifica continua dei **livelli di sicurezza dei fornitori e terze parti**
- **…**

+

Comportamenti

- **Vedi slide successiva**

AWARENESS E COMPORTAMENTI DEI DIPENDENTI

Il comportamento dei dipendenti può vanificare in pochissimo tempo ingenti investimenti in tecnologia

Il personale deve saper rilevare un tentativo di frode, contrastarlo e reagire velocemente.
In quasi tutti i casi i truffatori sfruttano la debolezza umana.

- **Programma di formazione obbligatoria (anche a squadre, con tecniche di gaming e classifiche). Aggiornamento dei casi d'uso,** le minacce sono in costante evoluzione
- **Coinvolgimento di_TUTTI i dependent - inclusi tempi determinati, a contratto, stage, etc.**
- **Riunioni o conference call periodiche**: non limitarti ad inviare emails o e learning
- Almeno **1 esercizio di crisi mngt l'anno** con le funzioni maggiormente a rischio
- **Formazione specifica al personale contabile e di tesoreria**

IN SINTESI, COSA RICORDARE

- **I rischi informatici sono in continua evoluzione**, necessario avere un “Sistema” di prevenzione / gestione solido e molto rapido nel reagire
- La sicurezza dell’azienda non basta, siamo legati in **ecosistemi complessi**: azienda / controllate / banche / fornitori / terze parti
- Alcune attività possono essere demandate **a società specializzate con expertise e track record**
- **La prevenzione ha un costo** che deve essere commisurata al rischio ma sarà crescente nel tempo; da tenere conto che **i rischi operativi / economici e reputazionali sono di gran lunga superiori**
- Il **comportamento dei dipendenti** può vanificare in pochissimo tempo ingenti investimenti in tecnologia

Associazione Italiana Tesorieri d'Impresa

Treasury & Finance Forum Day

Treasury Finance FORUM DAY

20 novembre 2020

Pleiadi International

grazie

Evento di

Associazione Italiana Tesorieri d'Impresa

Main sponsor

INTESA SANPAOLO

IMI CORPORATE & INVESTMENT BANKING

Con il patrocinio

CONFINDUSTRIA EMILIA
AREA CENTRO: le imprese di Bologna, Ferrara e Modena

Partner didattico

Academy ask

Sponsor

lexant STUDIO LEGALE

ask Advisory

BNL GRUPPO BNP PARIBAS

UniCredit Corporate & Investment Banking

Gruppo Bancario Cooperativo Iccrea

MF CENTRALE RISK

J.P.Morgan

TÜVRheinland®

MARZOTTO INVESTMENT HOUSE GROUP

WBADVISORS

nexi every day, every pay

4Planning

Piteco

pwc

DOCFINANCE

WesternUnion WU Business Solutions

Media partner

pleiadi international

MeetEasy by cs eventi

Seguici su

www.aiti.it

POST SCRIPTUM: PICCOLO BIGNAMI DEI BUONI COMPORTAMENTI

In caso di insolite richieste di bonifici	In caso di modifica di dati Bancari di un fornitore	Nel caso un tecnico Voglia aiutarti	Nel caso di Richiesta di informazioni
▪ Comunicalo ai tuoi responsabili ▪ Segui sempre il processo standard, indipendentemente dall'emergenza percepita ▪ Segui il pricincipio della separazione delle funzioni ▪ Controlla l'identità del tuo corrispondente usando i dettagli di contatto a te noti	▪ Controlla l'identità del tuo corrispondente usando i dettagli di contatto a te noti ▪ Controlla anche quando ricevi una richiesta di modifica dei contatti ▪ Fai molta attenzione se il conto è domiciliato all'estero e ai tuoi maggiori fornitori	▪ Contatta il tuo gestore di relazione (o il tuo fornitore di software) utilizzando I contatti a te noti ▪ Non dare accesso al tuo PC ▪ Non eseguire pagamenti test superiori a €1 ▪ Non fornire nessun codice a nessuno, nemmeno alla banca	▪ Non fornire informazioni a gente che non conosci ▪ Fai attenzione se qualcuno ti chiede informazioni contabili ▪ Controlla l'identità del tuo corrispondente usando i dettagli di contatto a te noti o attreverso la switchboard

POST SCRIPTUM: PICCOLO BIGNAMI DEI BUONI COMPORTAMENTI

Sui social networks E al di fuori dell'azienda

- Sii discreto sui social networks e al di fuori della tua azinenda per quanto riguarda il tuo ruole e le tue responsabilità
- Non pubblicare informazioni che potrebbero essere utili ai truffatori(organigrammi, notizie sul CEO, lettere, poteri di firma...)
- Se possibile, utilizza firmatari diversi da quelli che compaioni in documenti pubblici

Quando ricevi un'email

- Fai attenzione e controlla l'oggetto, il contenuto e l'indirizzo email del mittente
- Non cliccare sui link ricevuti nell'email: utilizza sempre l'app o il sito ufficiale; se per errore clicchi sul link, non inserire nessura informazione,
- Se possibile, non aprire gli allegati o non scaricare files; se apri il file, non autilizzare la modifica del contenuto

Quando usi Il tuo applicativo bancario

- Separa le funzioni, inserisci dei limiti, non utilizzare istruzioni cartacee
- Evita di connetterti dal tuo PC personale o dal tuo smartphone o da un rete pubblica di Wi-Fi
- Log off dalla tuo appliactivo ed elimina tutte le tue credenziali di accesso
- Non accedere quando c'è un sospetto di malware (finta pagina, problemi insoliti…); se in dubbio contatta il tuo gestore di relazione

Proteggi I tuoi sistemi informatici

- Aggiorna quotidianamente O.S. e gli anti virus
- RDP security (VPN o passwords)
- Sicurezza Website security
- Blocca le chiavi USB e i file condivisi
- Filtra le email e gli allegati (SPF, DKIM, DMARC)
- Testa i backup e aggiornali regolarmente
- Se possibile, encriptai i dati sensibili e utilizza TLS per email esterne