WINKLER & SANDRINI

Wirtschaftsprüfer und Steuerberater
Dottori Commercialisti - Revisori Contabili

Wirtschaftsprüfer und Steuerberater
Dottori Commercialisti e Revisori Contabili
Peter Winkler — Stefan Sandrini
Stefan Engele
Martina Malfertheiner — Oskar Malfertheiner
Stefano Seppi — Massimo Moser
Andrea Tinti — Michael Schieder
Stephanie Vigl — Roberto Cainelli
Rechtsanwalt - avvocato
Chiara Pezzi
Mitarbeiter – Collaboratori
Karoline de Monte — Iwan Gasser
Thomas Sandrini

Circolare

numero:	93i
del:	2019-11-27
autore:	Thomas Sandrini

A tutti i clienti con partita IVA

Email PEC fraudolenti

Negli ultimi mesi c'è stato un aumento nell'invio delle cosiddette "Phishing" PEC.(neologismo di "pesca", dalla parola inglese pescare). Si tratta di tentativi di ottenere dati personali tramite email falsificate al fine di commettere furti di identità. Più di recente, i messaggi PEC contenenti virus mascherati da file Excel sono stati inviati con maggiore frequenza.

1 "Phishing" tramite PEC

Le mail della PEC sono per lo più scritte in italiano senza errori, sembrano email "ufficiali" e a prima vista serie e hanno per oggetto ad es. "Invio File <XXXXXXXXXXXXXXXXXXX>". Per quanto riguarda i contenuti si fa riferimento al corretto sito web dell'Agenzia delle Entrate "*Per qualsiasi necessità di chiarimenti non rispondere a questa mail, ma utilizzare i tradizionali canali di assistenza presenti sul sito www.fatturapa.gov.it*" per dare l'impressione di serietà. Possono anche utilizzare i nomi e i numeri di identificazione delle fatture effettivamente inviate "Invio file ITYYYYYYYYYYYYYYYYYYY_1bxpz.XML.p7m, con identificativo <XXXXXXXX-XXXXXXXX>", le cui informazioni sono state spesso rubate prima da altri utenti.

La stessa PEC vi chiede di interrompere l'invio di tutte le future fatture elettroniche che emettete come di consueto e di inviarle ad un presunto indirizzo PEC della SDI: "Il nuovo indirizzo da utilizzare per inviare le prossime fatture al Sistema di Interscambio, fino fino ad un eventuale nuovo avviso, è YYY.YYY@pec.it". "L'utilizzo di un indirizzo diverso non garantisce il buon esito del recapito al destinatario".

Il truffatore di Internet cerca di invogliarvi ad inviare le fatture a lui e non più al "SDI" (Sistema di Interscambio dell'Agenzia delle Entrate). Lo scopo dei truffatori è quello di ottenere dati personali e di modificare singole parti della fattura, come l'IBAN, ecc. per reindirizzare i pagamenti sul conto del truffatore.

2 Virus tramite PEC

Anche queste email PEC hanno un aspetto molto simile alle email ufficiali e sono costruite come le email "phishing" appena descritte. Tuttavia, questa PEC vi chiede di consultare la fattura in allegato o, se non potete leggerla o aprirla, di disattivare i vari meccanismi di protezione del vostro computer (consentire tutte le macro di Office, scaricare dati da Internet,

ecc....). In realtà, l'allegato non contiene una fattura ma un virus, cryptolocker, o simili che permettono al truffatore di accedere ai vostri dati, criptarli o cancellarli.

3 Come ci si protegge da tali attacchi fraudolenti ?

Fondamentalmente, come per qualsiasi altra posta, è importante mostrare un sano scetticismo. Soprattutto se le email provengono da un mittente sconosciuto.

Con strane indagini o richieste di un mittente conosciuto, una breve indagine telefonica con il presunto mittente può creare chiarezza, poiché spesso il mittente della posta è falso e queste mail in realtà provengono da un'altra persona.

Aiuta anche a seguire alcune regole di base della sicurezza informatica:

- Sii sempre scettico e chiedi se hai dei dubbi;
- Controlla sempre i link e il mittente dell'email prima di cliccare su un indirizzo. Inoltre, è meglio non cliccare sul link presente nell'email, ma copiarlo nella barra degli indirizzi del browser per evitare il reindirizzamento verso un sito web diverso da quello visualizzato nell'email;
- Prima di cliccare su un link, è necessario verificare se l'indirizzo visualizzato è effettivamente lo stesso indirizzo Internet a cui il link conduce. Un controllo che può essere fatto facilmente: basta muovere il mouse sul link stesso;
- Evita di aprire allegati email sospetti ed evita di eseguire macro sui documenti di Office;
- In caso di dubbio, chiedete sempre aiuto al vostro reparto IT prima dell'apertura e chiedete loro di verificare se la posta, il link, l'allegato, ecc.... sono sicuri o meno;
- Non spegnete mai voi stessi il software antivirus, il firewall o altri meccanismi di sicurezza del vostro computer, anche se vi viene richiesto da una mail PEC "ufficiale".

Se, per qualsiasi motivo, avete aperto un allegato o un link sospettoso, informate immediatamente il vostro reparto IT - prima possono reagire a un'infezione (virus), meglio è.

Rimaniamo a disposizione per qualsiasi ulteriore chiarimento e porgiamo

cordiali saluti

Winkler & Sandrini
Dottori Commercialisti e Revisori Contabili