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

Rundschreiben

Nummer:	93
vom:	2019-11-27
Autor:	Thomas Sandrini

An alle Kunden mit MwSt. Nummer

Betrügerische PEC Mails

In den letzten Monaten kommt es wieder vermehrt zur Versendung von sogenannten „phishing" (Neologismus von „fishing", engl. für angeln) PEC's. Hierbei handelt es sich um Versuche, über gefälschte Mails, an persönliche Daten zu gelangen, um damit Identitätsdiebstahl zu begehen. Zuletzt wurden auch wieder häufiger PEC-Mails mit Viren, getarnt als Excel Dateien, versendet.

1 „phishing" über PEC

Die PEC Mails sind meist in fehlerfreiem Italienisch verfasst, sehen auf den ersten Blick offiziell und seriös aus und haben einen Betreff wie *„Invio File <XXXXXXXXXX>".* Inhaltlich verweisen sie u.a. auf die richtige Webseite der Agentur der Einnahmen *„Per qualsiasi necessità di chiarimenti non rispondere a questa mail, ma utilizzare i tradizionali canali di assistenza presenti sul sito www.fatturapa.gov.it",* um einen seriösen Eindruck zu erwecken. Unter Umständen verwenden sie sogar die Namen und Identifikationsnummern effektiv versendeter Rechnungen *„Invio file ITYYYYYYYYYY_1bxpz.XML.p7m, con identificativo <XXXXXXXXXX>",* deren Informationen oft im Vorfeld bei anderen Benutzer gestohlen wurden.

Die PEC selbst fordert Sie auf, alle zukünftigen elektronischen Rechnungen, welche Sie ausstellen, nicht mehr wie gewohnt zu versenden, sondern an eine vermeintliche PEC Adresse des SDI zu senden: *„Il nuovo indirizzo da utilizzare per inviare le prossime fatture al Sistema di Interscambio, 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."*

Der Internet Betrüger versucht hierbei, Sie dazu zu verleiten, die Rechnungen an ihn und nicht mehr an das „SDI" (Sistema di Interscambio der Agentur der Einnahmen) zu senden. Ziel der Betrüger ist es in den Besitz persönlicher Daten zu gelangen und einzelne Bestandteile der Rechnung wie z.B. IBAN usw… zu verändern, um Zahlungen auf das Konto des Betrügers umzuleiten.

2 Viren über PEC

Auch diese PEC Mails sehen offiziellen Mails äußerst ähnlich und sind wie die eben beschriebenen „fisching" Mails konstruiert. Diese PEC fordert Sie jedoch auf, die Rechnung im

Anhang zu konsultieren bzw. falls Sie diese nicht lesen oder öffnen können diverse Schutzmechanismen Ihres Computers zu deaktivieren (alle Office-Makros zulassen, Daten aus dem Internet nachladen usw.…). In Wirklichkeit enthält der Anhang keine Rechnung sondern einen Virus, Cryptolocker o.ä.; welcher dem Betrüger Zugriff auf Ihre Daten gewährt, diese verschlüsselt oder löscht.

3 Wie kann man sich vor diesen Betrugsversuchen schützen?

Grundsätzlich gilt es, wie bei jeder anderen Mail auch, eine gesunde Skepsis an den Tag zu legen. Insbesondere dann, wenn sie von einem unbekannten Absender stammen.

Bei sonderbaren Anfragen oder Aufforderungen eines bekannten Absenders kann eine kurze telefonische Rückfrage bei dem vermeintlichen Absender Klarheit schaffen, da oftmals der Absender des Mails gefälscht wird und diese Mails in Wirklichkeit von einer anderen Person stammt.

Es hilft auch einige Grundregeln der Computersicherheit zu befolgen:

- Seien Sie grundsätzlich skeptisch und fragen sie bei Zweifel nach;
- Überprüfen Sie immer Links und Absender der E-Mail bevor Sie auf eine Adresse klicken. Zudem ist es besser, den Link im Mail gar nicht anzuklicken, sondern in die Adressleiste des Browsers zu kopieren, um eine Umleitung auf eine andere Webseite als die im Mail angezeigte zu verhindern;
- Bevor Sie auf einen Link klicken, sollten Sie überprüfen, ob die angezeigte Adresse wirklich die gleiche Internetadresse ist, zu der der Link führt. Eine Überprüfung, die auf einfache Weise durchgeführt werden kann: fahren Sie einfach mit der Maus über den Link selbst;
- Vermeiden Sie das Öffnen verdächtiger E-Mail-Anhänge und vermeiden Sie bei Office-Dokumenten die Ausführung von Makros;
- Bitten Sie bei Zweifeln immer vor dem Öffnen Ihre EDV Abteilung um Hilfe und bitten Sie sie um Überprüfung, ob das Mail, der Link, der Anhang etc… sicher sind oder nicht;
- Schalten Sie niemals in Eigenregie Ihre Antivirus Software, Firewall oder sonstige Sicherheitsmechanismen Ihres Computers aus, auch nicht dann, wenn Sie von einer „offiziellen“ PEC-Mail dazu aufgefordert werden.

Sollten Sie trotzdem aus welchen Gründen auch immer, einen verdächtigen Anhang oder Link geöffnet haben, machen Sie dies umgehend Ihrer EDV Abteilung bekannt - je früher diese bei einer Infektion (Virus) reagieren kann, desto besser.

Für weitere Fragen stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen

Winkler & Sandrini
Wirtschaftsprüfer und Steuerberater