Run my Accounts

Cybersecurity

Mitarbeiter-Schulung

Agenda

1) Einleitung
2) Gefahren
3) Wie schützen wir uns?

Einleitung

Run my Accounts

Zunehmende Bedrohungslage

- Im Internet tobt ein Krieg: https://cybermap.kaspersky.com/de
- Erstes Halbjahr 2021:
  - Cyber-Attacken: +29%
  - Ransomware: +93%
- Beispiele:
  - Solarwinds
    - Praktikant hat Passwörter veröffentlicht
    - Vertrauliche Daten in tausenden Firmen entwendet
  - Colonial Pipeline
    - Ransomware
    - Ölversorgung an US-Ostküste lahmgelegt
  - Kaseya
    - Ransomware
    - Kassenlösung von tausenden Retailern lahmgelegt, Schwedischer Coop während musste 800 Läden während Tagen schliessen

Run my Accounts

Social Engineering: wir alle sind einfache Opfer!

https://youtu.be/F7pYHN9iC9I

Run my Accounts

Wer greift an?

- Cyberkriminelle
  - Erpresser
  - Handel mit Informationen
  - Finanzbetrüger
- Geheimdienste
- Hacktivisten / Cyberaktivisten

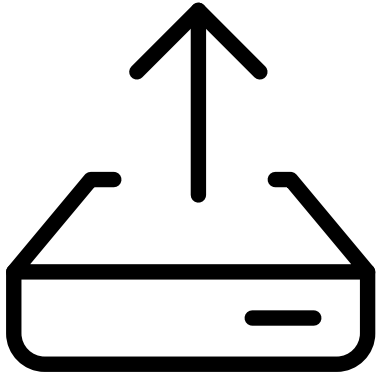
Run my Accounts

Gefahren

Run my Accounts

Daten-Diebstahl

- Diebstahl von:
  - Geschäftsgeheimnissen
  - Vertrauliche Kundendaten
  - Geistiges Eigentum, Code
- Gefahr geht aus von:
  - Auskünfte eigener Mitarbeiter
  - Schlecht gewartete Server
  - Software-Fehler
  - Leicht angreifbare Backups / Test-Server
- Ziel des Hackers:
  - Erpressung mit Veröffentlichung
  - Verkauf an interessierte Kreise / Kunden / Konkurrenten



Run my Accounts

Ransomware

- Was ist Ransomware?
  - «Verschlüsselungs-Trojaner».
  - Dateien auf Computer und im Netzwerk werden verschlüsselt.
  - Aktivierung oft per Doppelklick auf ein Mail-Attachment.
- Ziel des Angreifers:
  - Erpressung von viel Geld (meist per Bitcoin zahlbar) gegen Herausgabe des Schlüssels.

Quelle: Wikipedia

CEO Betrug

- Szenario:
  - Angreifer gibt sich als leitender Angestellter aus und will Mitarbeiter / Treuhänder zum Transfer eines grösseren Geldbetrages veranlassen.
  - Angreifer beschafft sich im Vorfeld Informationen über die internen Gegebenheiten der Firma.
  - Internationale Zahlung unter Dringlichkeit / Verschwiegenheit
- Empfehlungen:
  - Telefonisch beim Kunden nachfragen
  - Traue keiner E-Mail!

Run my Accounts

E-Banking Schadsoftware

- Vorgehen:
  - Schadsoftware manipuliert E-Banking und löst Transaktionen aus.
  - Einschleusen per Gratis-Download-Button, E-Mail-Anhang, Webseiten-Virus.
  - Offline-Zahlungs-Software wird manipuliert.
- Vermeidung:
  - 2 Faktoren Authentifizierung
  - Kollektiv-Vollmacht im E-Banking

Run my Accounts

Phishing

- Phishing = Password + Harvesting + Fishing
  - Betrüger wollen an vertrauliche Daten gelangen.
    - Usernamen / Passwörter
    - Kreditkarten-Daten
  - Ausnutzen der Hilfsbereitschaft des Opfers.
  - Masche: Zugangsdaten nicht mehr sicher / aktuell. Diese sollen aufdatiert werden.
  - Opfer gelangt auf ein Gefälschtes Web-Formular, welches wie Original-Webseite aussieht und gibt vertrauliche Daten ein.
- Gegenmassnahmen:
  - URL / Zertifikat überprüfen
  - 2 Faktor-Authentifizierung
  - Eine Bank holt nie Login-Daten ein!

Re: Google-Vergütung

Von: **GOOGLE.COM** | test@gov.ru

An: **Recipients** | test@gov.ru

Hallo Begünstigter,

Montag, 9.

Bei der kürzlich abgeschlossenen Google Online-Verlosung 2021 erhalten Sie als aktiver Nutzer den Be
von 950,000 GBP. Bitte antworten Sie mit den Details unten für weitere Informationen und bestätigen Sie
Gewinncode lautet GFP/875/GPWIN/EU.

(1) Ihre Adresse....
(2) Handynummer....
(3) Nationalität....
(4) Vollständiger Name....
(5) Beruf....
(6) Geschlecht....
(7) Sprechen Sie Englisch?

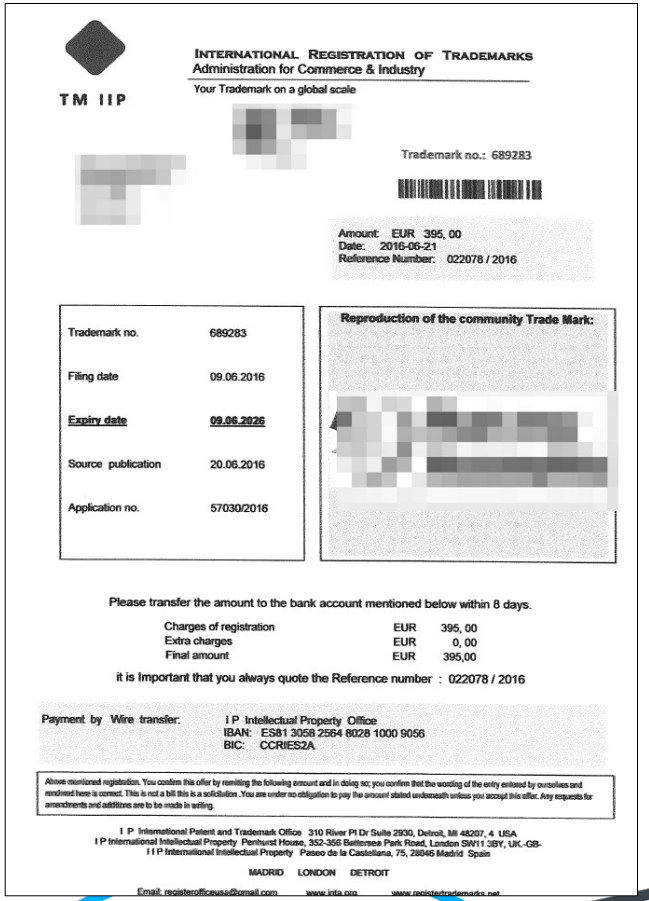
Wir beglückwünschen Sie im Namen des Google-Teams.

Herr Larry, Google Online Director
Buckingham Palace Road,
WC2H 8AG London, Großbritannien.

Run my Accounts

Fake Rechnung

- Szenarien:
  - Rechnung für eine Leistung, die nicht vereinbart wurde.
  - Rechnung mit falscher IBAN / QR-Rechnung / Einzahlungsschein.
  - Hinweis, dass für künftige Zahlungen ein anderes Konto verwendet werden soll.
- Gegenmassnahmen:
  - Prozess zur Rechnungsprüfung
  - Prozess zur Zahlungsfreigabe
  - Stammdatenanpassungen nur unter Rückfrage an Lieferanten



TM IIP

INTERNATIONAL REGISTRATION OF TRADEMARKS
Administration for Commerce & Industry
Your Trademark on a global scale

[redacted]

Trademark no.: 689283

[redacted]

Amount: EUR 395, 00
Date: 2016-06-21
Reference Number: 022078 / 2016

Trademark no.	689283
Filing date	09.06.2016
Expiry date	09.06.2026
Source publication	20.06.2016
Application no.	57030/2016

Reproduction of the community Trade Mark:

[redacted]

Please transfer the amount to the bank account mentioned below within 8 days.

Charges of registration	EUR	395, 00
Extra charges	EUR	0, 00
Final amount	EUR	395,00

it is Important that you always quote the Reference number : 022078 / 2016

Payment by Wire transfer: I P Intellectual Property Office
IBAN: ES81 3058 2564 8028 1000 9056
BIC: CCRIES2A

Above mentioned registration. You confirm this offer by remitting the following amount and in doing so; you confirm that the wording of the entry entered by ourselves and rendered here is correct. This is not a bill this is a solicitation .You are under no obligation to pay the amount stated underneath unless you accept this offer. Any requests for amendments and additions are to be made in writing.

I P International Patent and Trademark Office 310 River Pl Dr Suite 2930, Detroit, MI 48207, 4 USA
I P International Intellectual Property Penhurst House, 352-356 Battersea Park Road, London SW11 3BY, UK.-GB-
I I P International Intellectual Property Paseo de la Castellana, 75, 28046 Madrid Spain

MADRID LONDON DETROIT

Email: registeroffices@gmail.com www.inta.org www.registertrademarks.net

Schadsoftware nach Anruf

- Vorgehen der Betrüger:
  - Brief- oder Paketzusteller will Versandpapiere visieren lassen / Bank will E-Banking Update machen.
  - Im Telefongespräch wird mitgeteilt, dass Dokumente per E-Mail zugestellt werden.
  - Mitarbeiter erhält E-Mail noch während des Anrufs und wird aufgefordert, den Anhang (oft ein vermeintliches PDF – jedoch Schadsoftware) zu öffnen.
- Massnahmen:
  - Gesundes Misstrauen!
  - Am Telefon nie unter Druck setzen lassen!

Run my Accounts

Was können wir dagegen tun?

Run my Accounts

Sicherer Umgang mit E-Mails

- ACHTUNG: E-Mail Absender können ganz einfach gefälscht werden!
- Erkennen von Phishing-E-Mails:
  - Oft kleine Rechtschreibfehler und Unstimmigkeiten.
  - Links zu verdächtigen Webseiten.
  - Falsche Fehlermeldungen, welche die Neugier des Empfängers triggern.
- Grosse Versprechungen:
  - Sie haben gewonnen!
  - Zustellung eines Paketes
  - Grosser Deal in Aussicht

Sicherer Umgang mit Passwörtern

- Strikte Verwendung Passwort-Manager wie 1password oder Bitwarden – auch privat!
- Komplizierte Passwörter mit Passwort-Generator in Passwort-Manager erstellen.
- Anforderungen an ein gutes Passwort:
  - Lang
  - Kleine / grosse Buchstaben, Sonderzeichen, Ziffern
  - Keine Namen, Daten, Wörter aus Wörterbüchern
  - Keine gängigen Wiederholungs- und Tastaturmuster (1234, abcd, …)
- Nie das selbe Passwort für verschiedene Dienste verwenden.
- Wenn möglich immer 2-Faktor-Authentifzierung verwenden.
  - SMS
  - Google Authentificator
  - Yubico

Run my Accounts

Umgang mit Dateien

- Alle Dateien möglichst auf einem Server speichern, auf dem regelmässig ein lokal getrenntes und nicht vernetztes Backup erstellt wird.
  - Z.B. Anwendung von Google Drive Desktop mit Streaming-Funktion – Backup der Dateien in geeigneter Infrastruktur.
- Zugriff auf Dateien nur auf Need-to-Know-Basis erteilen.
  - Je restriktiver der Zugriff auf die Dateien, desto kleiner das Risiko.

Run my Accounts

Software-Updates installieren

- Immer neueste Software-Updates installieren:
  - Betriebs-System Updates und Patches
  - Neue Software-Versionen
- Vorsicht bei Software, die schon lange kein Update mehr erhalten hat.

Run my Accounts

MISSTRAUEN!!! – MISSTRAUEN!!! – MISSTRAUEN!!!

- Immer kritisch und misstrauisch sein.
- Beim geringstem Zweifel bei Kunden, Kollegen, … rückfragen.
- Passwörter nie mit jemandem teilen.
- Login-Daten weder per Telefon mitteilen noch per E-Mail versenden.
- Besonders kritisch sein bei bei E-Mail-Anhängen, schlecht formulierten Mails, unbekannten Absendern, Links auf externe Downloads.
- Nicht auf Druck reagieren (dringende / vertrauliche Anfragen / Nötigungen / …).
- Office Dokumente: Makros nie aktivieren.