Die Wirtschaft

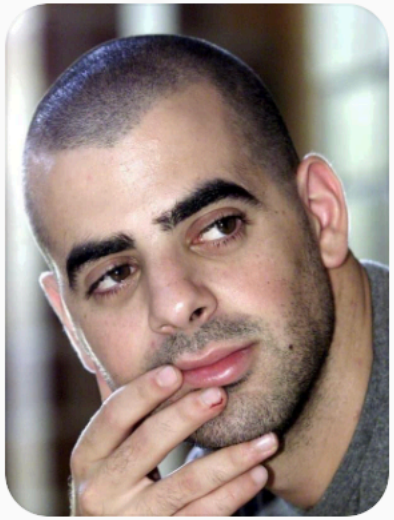
Prutz-Faggen

Was bringt einen Menschen dazu, einem völlig
Fremden absichtlich Schaden zuzufügen?

Ist es Langeweile? Ist es Neugier? Ist es Wut?
Vielleicht eine persönliche Kränkung?
Oder geht es schlicht ums Geld?

We did it for the power!

Weil wir die Macht hatten,
es zu machen.



**Ehud Tannenbaum (1979)*

Der israelische Hacker mit dem Pseudonym *The Analyzer* war 1998 etwa 18 Jahre alt. Gemeinsam mit zwei 16-jährigen Amerikanern war er an einer Angriffswelle auf Computersysteme des US-Verteidigungsministeriums beteiligt.

Drei Täterwelten

01

Emotionale Täter

Anerkennung, Rache, Machtgefühl

02

Cyberkriminelle

Geld, Konten, Erpressung

03

Staatliche Akteure

Spionage, Einfluss, Sabotage

Das Opfer ist manchmal gezielt ausgewählt. Bei Massen-Phishing ist es oft austauschbar.

Internationale Netzwerke



1. Anonymous – Die digitalen Aktivisten

Entstanden um 2003, international. Ein loses Kollektiv ohne zentrale Führung. Bekannt für Angriffe auf Scientology, staatliche Einrichtungen und Unternehmen. Häufig politisch oder ideologisch motiviert.

Motiv: Protest, Aufmerksamkeit, Aktivismus.

2. LulzSec – Hacken aus Spaß

Besonders aktiv 2011. Angriffe auf Sony, PBS und andere Organisationen. Der Name stammt von „Laughing Out Loud" und „Security". Die Gruppe wollte Sicherheitslücken bloßstellen, provozieren und sich über ihre Opfer lustig machen.

Motiv: Spaß, Provokation, Geltungsdrang.

3. Chaos Computer Club (CCC) – Die ethischen Hacker

Gegründet 1981 in Deutschland. Eine der ältesten und bekanntesten Hackervereinigungen Europas. Setzt sich für Datenschutz, Informationsfreiheit und IT-Sicherheit ein. Bekannt für öffentlichkeitswirksame Demonstrationen von Sicherheitslücken.

Motiv: Aufklärung, Datenschutz, Verbesserung der Sicherheit.

Wichtig: Der CCC ist keine Cybercrime-Bande.

4. LockBit – Die digitalen Erpresser

Seit 2019 bekannt. Internationales Ransomware-Netzwerk, das Unternehmen und Behörden mit Verschlüsselung und der Veröffentlichung gestohlener Daten erpresst. 2024 wurden Teile der Infrastruktur durch internationale Ermittlungen zerschlagen.

Motiv: Geld, Erpressung, organisierte Kriminalität.



5. Lazarus Group – Hacker im Staatsauftrag

Nordkorea zugeschriebene Hackergruppe. Bekannt durch den Angriff auf Sony Pictures 2014, den WannaCry-Angriff 2017 und große Kryptowährungsdiebstähle.

Motiv: Finanzierung des Regimes, Spionage, politische Interessen.



6. Fancy Bear (APT28) – Die Cyber-Spione

Russland zugeschriebene Gruppe, die mit dem Militärnachrichtendienst GRU in Verbindung gebracht wird. Bekannt für Spionage, Phishing-Kampagnen und Angriffe auf politische Institutionen, darunter der Deutsche Bundestag 2015.

Motiv: Spionage, geopolitischer Einfluss, Informationsbeschaffung.

Psychologie des Täters

Langeweile	Reiz und Grenzüberschreitung
Kränkung	Vergeltung nach erlebter Demütigung
Geltungsdrang	Status in einer Gruppe
Macht	Kontrolle über fremde Systeme
Gier	Angriff als Geschäftsmodell

Ein Angriff kann mehrere Motive verbinden.

Angriffe im Alltag

PHISHING	Zugangsdaten oder Informationen
SMS / ANRUF	Täuschung über Smishing oder Vishing
SCHADSOFTWARE	Anhang oder Download öffnet die Tür
KONTOÜBERNAHME	Nachrichten kommen vom echten Konto
RECHNUNGSBETRUG	Bankverbindung wird ausgetauscht

Fünf Hebel der Täuschung

ZEITDRUCK	„Nur noch heute“
ANGST	„Ihr Konto wurde gesperrt“
AUTORITÄT	„Hier spricht das Ministerium“
BELOHNUNG	„Sie erhalten eine Rückzahlung“
HILFSBEREITSCHAFT	„Ich brauche dringend deine Hilfe“

Unter Druck prüfen Menschen weniger sorgfältig.

Die Warnsignale

1	Absenderdomain	Sachfremde Domain statt bmf.gv.at
2	Linkziel	Button führt auf eine andere Website
3	Psychologie	Belohnung, Autorität und Zeitdruck
4	Bankdaten	Ungewöhnliche Aufforderung zur Prüfung
5	Kontext	Unpersönliche Anrede und unpassender Empfänger

Die offizielle Website selbst öffnen. Nie über den Mail-Link anmelden.

Ein gültiges Siegel der falschen Firma

DKIM: PASS

Die fremde Domain hat die Nachricht korrekt signiert.

Das beweist nicht, dass die Nachricht vom Finanzministerium stammt.

Technisch korrekt kann trotzdem betrügerisch sein.

Die Prüfroutine

STOPP

Zeitdruck unterbrechen
Nicht klicken oder zahlen

PRÜFEN

Absender, Linkziel
und Anliegen kontrollieren

BESTÄTIGEN

Website selbst öffnen
Bekannten Kontaktweg
nutzen

Eine kurze Pause schützt besser als hektische Gewissheit.

Wenn bereits etwas passiert ist

01 Vorgang abbrechen

02 Passwort über die echte Website ändern

03 Andere Konten mit demselben Passwort absichern

04 Sitzungen abmelden und zweiten Faktor aktivieren

05 Bei Zahlungen sofort die Bank informieren

06 Beweise sichern und Hilfe holen

Fünf Dinge, die bleiben sollen

1. Dringlichkeit ist ein Warnsignal.
2. Der sichtbare Absendername beweist nichts.
3. Professionelles Design beweist nichts.
4. Zahlungsänderungen immer unabhängig bestätigen.
5. Nach einem Fehler sofort handeln.

Die kurze Pause vor dem Klick

STOPP

PRÜFEN

BESTÄTIGEN

Fragen?