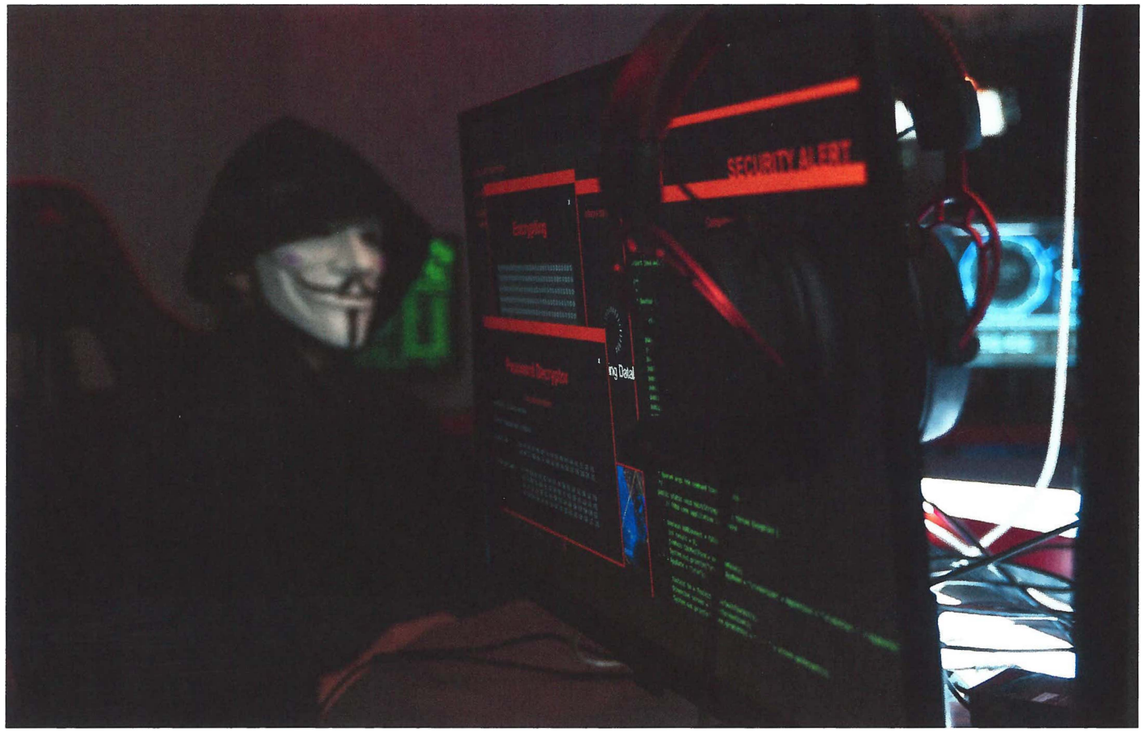


Was ist Social Engineering?

Das Thema Social Engineering ist leider nur wenigen Unternehmern bekannt, was genau kann man sich darunter vorstellen? können Sie uns den Begriff genauer erklären?

Social Engineering ist ein breiter Begriff, das einfachste ist aber wohl zu verstehen, dass man bei diesem Begriff immer die menschlichen Schwächen einer 3. Person nutzt um etwas zu erreichen. Sei es mit vorgängiger tiefer Recherche über deren Vorlieben, oder auch mit gezielter Falschinformation zu manipulieren um ein Ziel zu erreichen. Die bekanntesten sind wohl der Enkeltrick bei älteren Leuten oder auch das Mail vom Prinz aus Saudiarabien um ihm sein Geld zu beschaffen.

Was sind die Risiken im Sozialengineering?

Je nach Vorbereitung und Informationen über das Opfer mittels Instagram, Facebook oder sonstiger Quellen, fällt es dem Opfer extrem schwer zu erkennen, dass es manipuliert wird. Daher merkt man es erst, wenn die Falle zugeschnappt ist.

Ein grosser Risikofaktor ist der Mensch, aber wieso ist dies so und warum findet dies statt?

Wie soll ich sagen, der Mensch ist fast immer das schwächste Glied in der Kette, warum soll ich mich dann nicht genau darauf fokussieren?

Ein Projekt, bei welchem auch Mount10 mitwirkt, ist die Plattform www.kmuschutz.ch. Um was geht es auf dieser Webseite, und dem Projekt genau?

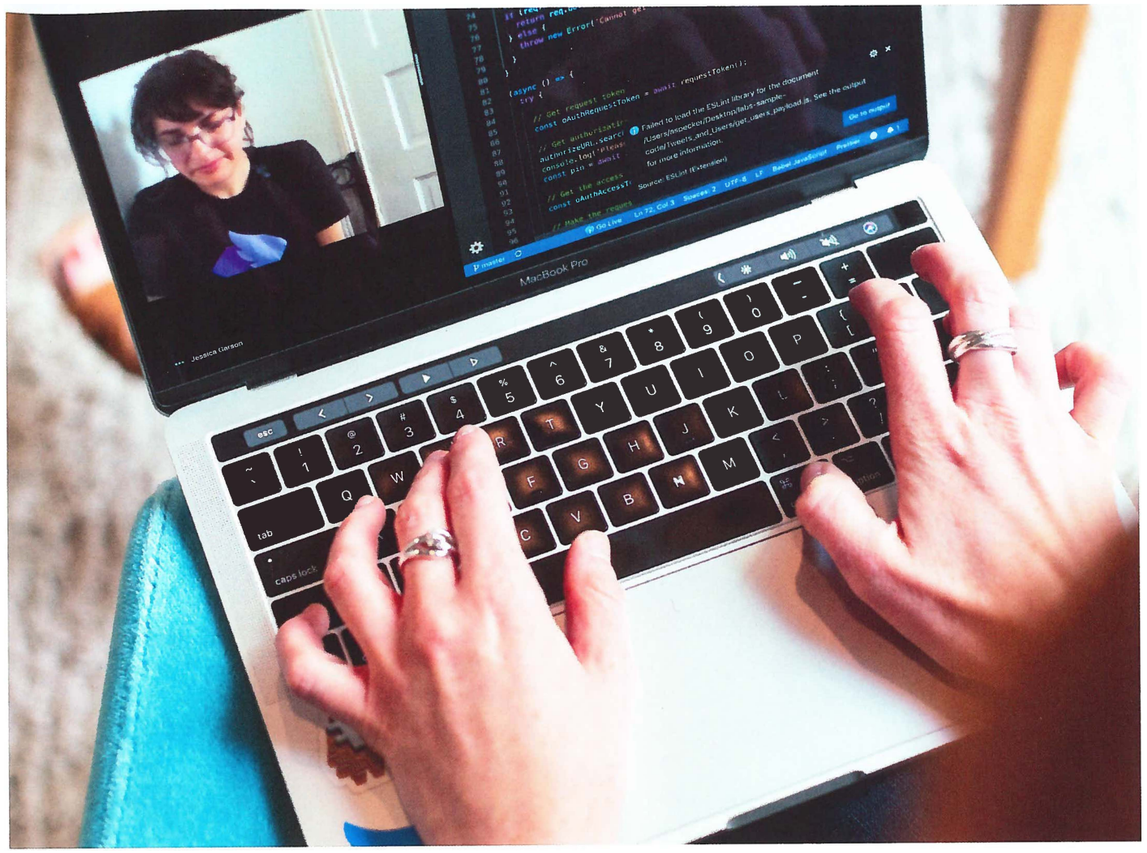
Leider sind immer häufiger auch KMU's aller Art von Verschlüsselungstrojanern betroffen. Diese KMU's haben nicht die Ressourcen, also das Geld , das Know-how oder sei es auch nur die Zeit, sich vertieft mit dem Schutz vor Ransomware zu befassen. Daher haben wir uns als unabhängige Trägerschaft von namhaften Firmen zusammengetan um einen einfachen verständlichen Leitfaden für den Schutz der KMU's zu erstellen. 6 Einfache, verständliche Massnahmen, die, wenn befolgt, ein KMU vor dem Schlimmsten bewahren.

Mir ist aufgefallen, dass auf der Website mehrere Sicherheitsunternehmen zusammenarbeiten, die jedoch in Konkurenz miteinander stehen, zeig das die Einigkeit zur Gefährlichkeit der Hackerangriffe?

Das ist ein sehr guter Punkt. Neben der Erkenntnis wie gefährlich die Angriffe sind, ist es auch ein Zeichen der Neutralität und Unabhängigkeit. Keine der Massnahmen zielt auf die Technologie eines Unternehmens ab, denn es geht um den Inhalt und nicht um das beste Tool, die beste Technologie oder mehr Umsatz bei der Trägerschaft. Unser erklärtes Ziel mit dieser Non-Profit Initiative ist die Hürde für Erpresser so hoch zu machen, dass die Schweizer KMU's kein lohnenswertes Ziel mehr sein werden.

In der Schweizer KMU Welt ist es leider immer noch so, dass viele kleinere Unternehmen der Meinung sind, zu klein und unbedeutend zu sein für Hacker Angriffe auf ihre Daten, wie sehen sie das?

Solange sie als KMU einen einzigen



Lohn für einen Mitarbeiter bezahlen, sind sie ein lohnenswertes Ziel. Die Grösse der KMU ist dem Angreiffer egal, er kann nur gewinnen, er lässt ja eine Schadsoftware für sich arbeiten. Gerade weil die kleinen KMU's sich nicht genug schützen können, sind genau diese die grossen Verlierer.

Ein Satz den wir immer wieder zu hören bekommen: „ich habe eine Antiviren Software, somit bin ich geschützt. Wie sehen Sie das, bietet eine Antivieren Software so viel Schutz wie da behauptet wird?

Eine der 6 Massnahmen ist genau die von Ihnen beschriebene Antiviren Software, die kann viel verhindern, aber nicht alles. Daher die restlichen 5 Massnahmen. Wir haben viel Zeit und Energie in die möglichst einfache Verständlichkeit und die Erarbeitung des absoluten Minimums gesteckt. Wenn es mit obigem gelöst wäre, hätten wir uns viel Zeit und Energie sparen können.

Ein weitverbreiteter Irrtum unserer Gesellschaft ist die Meinung „ich verwende ein IPhone, das ist doch eh nicht hackbar." wie sehen Sie das?

In der Geschäftswelt sind Smartphones nicht mehr wegzudenken, sie sind aber nicht dazu da Geschäftsdaten zu speichern oder zu erstellen. Sie werden vor allem als mobiles «Sichtfenster» für Systeme genutzt die auf Servern oder in der Cloud arbeiten. Es ist eine der Voraussetzungen, dass Smartphones möglichst sicher sind, das hat aber leider wenig Einfluss darauf wie verwundbar Ihre Firma im Internet wirklich ist.

Wie sehen Sie die aktuelle Situation mit den Hackerangriffen und wie kann man das Ihrer Meinung nach ändern?

Aufgrund der Statistiken der NCSC des Bundes (ehemals MELANI), werden kontinuierlich mehr Angriffe verzeichnet. Das Business mit Schutzgeld-Erpressung scheint zu boomen, ob das auch der Grund hinter dem Anstieg des Bitcoin Wertes ist kann nur vermutet werden. Eine Umkehr dieses Trendes kann man mainer meinung nach nur erreichen, wenn man den Markt austrocknet, als sich jede und jeder soweit schützt, dass er kein lohnenswertes Ziel mehr ist. Unserer Meinung nach ist die Swiss Cyber Defence – DNA Initiative ein gutes Hilfsmittel auf diesem Weg: Neutral, klar, einfach, breit abgestützt und kostenlos!

Thomas Liechti ist CEO der MOUNT10 AG und Initiant der Swiss Cyber Defence – DNA Initiative.