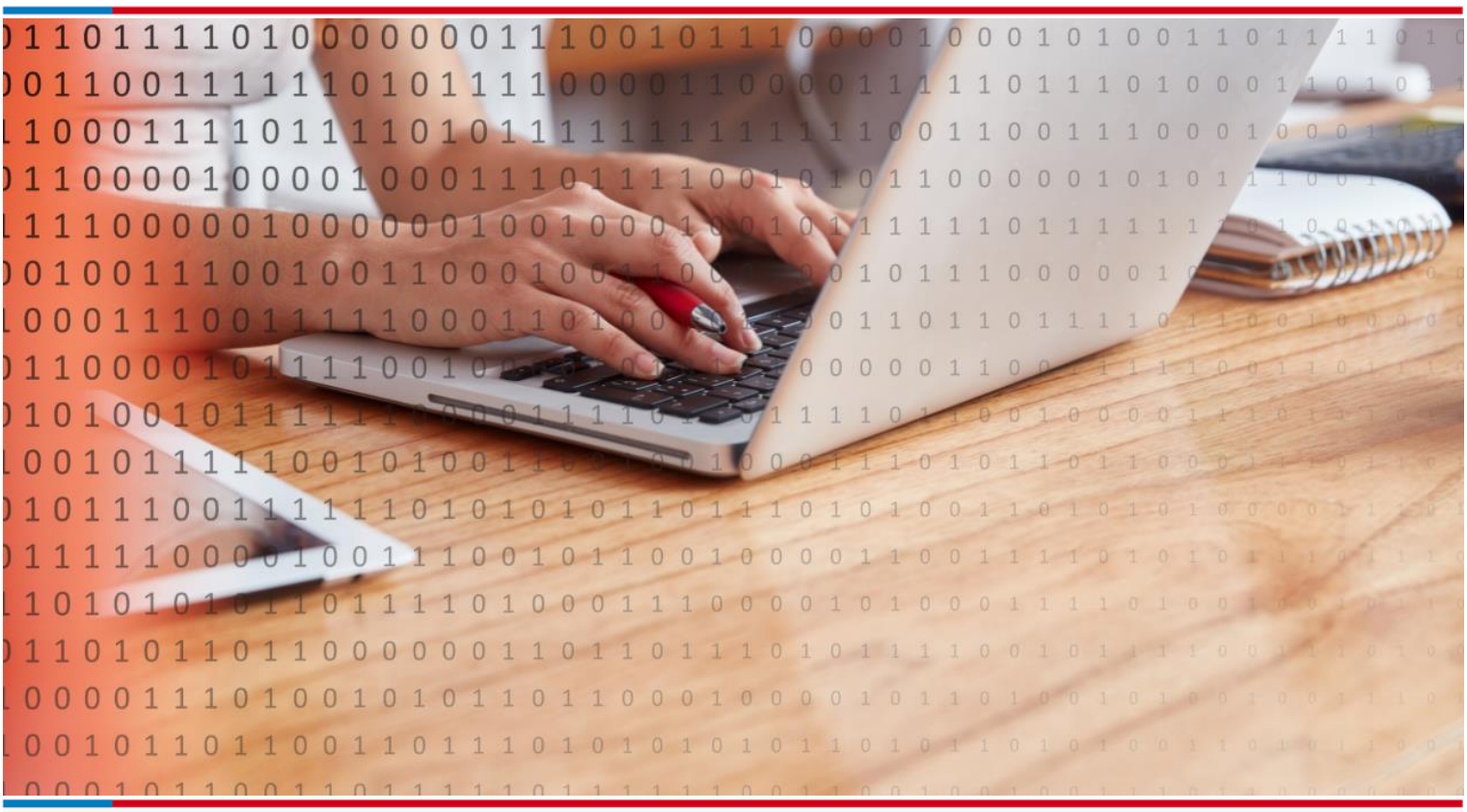
Der Awareness-Horizont – den Mindset managen



Autor: Dr. Michael Wolfensberger, Joël Bühler

Wir haben es alle immer und überall mit Risiken zu tun. Privat wie beruflich. Beim Autofahren, im Tram, in der Freizeit ebenso wie im Umgang mit Arbeitsgeräten, die nun einmal zumeist Computer sind oder sich auf IT-Technologie stützen. Die meisten Risiken bemerken wir gar nicht, andere nehmen wir einfach in Kauf und gegen wieder andere ergreifen wir tatsächlich Massnahmen, wenn sie auf unserem persönlichen Radar sind – innerhalb des Awareness-Horizonts.

Alles eine Frage der Wahrnehmung.

Der Awareness-Horizont

Diejenigen Risiken, die wir wegen ihrer Auswirkungen auf uns persönlich hoch genug bewerten, dass wir zu unserem Selbstschutz Massnahmen ergreifen, bleiben «auf unserem Radar». Sie sind damit innerhalb unseres persönlichen Awareness-Horizonts. Es ist die Bewertung der individuellen Konsequenzen, die uns antreibt, unser Verhalten zu ändern. Man merkt sich immer, wo man schon mal mit dem Auto geblitzt wurde oder sonst irgendwie einen direkten Schaden erlitten hat. Auch in Bezug auf unsere private und berufliche Nutzung von IT haben wir einen individuellen Awareness-Horizont. Der kann unbeabsichtigtes Löschen von Daten, Verlust von Datenträgern, Virenbefall oder Identitätsdiebstahl umfassen. Dagegen wehrt sich jede:r einzelne Nutzer:in nach besten Kräften, wenn es ihn direkt und spürbar betrifft. Sicherheit wird dabei ganz individuell als «Abwesenheit intolerabler Risiken» erlebt.

Verantwortungsdissoziation

In Firmen oder Organisationen allgemein reicht dieser individuelle Horizont jedoch nicht aus. Dort werden Prozesse und damit auch Daten arbeitsteilig bearbeitet. Die Lehren, die jede:r Einzelne aus IT-Sicherheitszwischenfällen zieht, sind definitiv nicht hinreichend, um eine Organisation vor Schaden zu bewahren. Einerseits kommt es bei wachsender Grösse der Organisation zu einer ebenfalls wachsenden Verantwortungsdissoziation, wo jede:r Einzelne glaubt, ein:e andere:r werde schon dafür sorgen, dass nichts passiert. Andererseits bedeutet Aufgabenteilung auch Wissensteilung, und so kommen Angreifer:innen und Datendieb:innen oft gänzlich unbemerkt davon, weil allfällig verdächtige Unregelmässigkeiten einfach unbemerkt bleiben oder von jeweiligen IT-Anwender:innen mangels besseren Wissens anderen vertrauenswürdigen Mitarbeiter:innen zugeschrieben werden, die vermeintlich «vielleicht etwas anders», aber bestimmt nichts falsch gemacht haben.

Schliesslich gibt es immer noch den Mythos Maschine, der mit Firewalls, Virenscannern und anderen Wunderwaffen der IT für Sicherheit und Ordnung sorgt. Aber dieser Mythos hält nicht, was er verspricht. Und auch der CISO kann nicht wie der Erzengel St. Michael mit Schild und Schwert die Hacker abwehren. Zum Schutz von Mensch und Maschine braucht es den Mindset in den Köpfen aller. Weil es jede:n betrifft. Jede:r muss sich und den Nachbar:innen Sorge tragen – dann klappt es mit der Sicherheit.

Bewusstsein und System

Es ist notwendig, der Bedrohung mit einem systematischen Sicherheitsansatz zu begegnen, denn die individuellen Awareness-Horizonte der Mitarbeiter:innen müssen aufeinander abgestimmt, kombiniert und koordiniert – kurz: gemanaged – sein, um wirksamen Schutz bieten zu können. Erst wenn jede:r Mitarbeiter:in versteht, dass ein unbedachter persönlicher Klick oder ein Datendiebstahl fernab seiner eigenen Organisationseinheit ihn ganz persönlich innert Wochen den Job kosten kann, ist der Awareness-Horizont angemessen abgesteckt. Dieser Mindset ist wesentlich für den Schutz aller. Ob gestohlene Blaupausen oder Datenlecks, die in der Presse erscheinen: Die Angreifer und die Konkurrenz freuen sich, die Organisation leidet.

Ob NIST, ISO 27000, die VdS 10’000-Richtlinie aus Deutschland, BSI-Grundschutz, die einfache IT-Sicherheits-Checkliste der ISSS oder ein beliebiges anderes Modell - überall sind Schulungs- und Awareness-Massnahmen dabei, die das Sicherheits-Bewusstsein der Mitarbeiter:innen schärfen sollen. Diese Massnahmen sorgen dafür, dass die Awareness-Horizonte der einzelnen Mitarbeiter:innen angemessen erweitert, sinnvoll miteinander verknüpft und so zu einem zusätzlichen wirksamen und gesamtheitlichen Sicherheitssystem verbunden werden. Die Mitarbeiter:innen werden so zu einem kompetenten Teil des IT-Schutzes. Sie haben sogar noch Freude und schöpfen Motivation daraus, erfolgreich ein Phishing-Mail oder eine andere Bedrohung erkannt und gemeldet zu haben. Dazu muss nur jede:r verstehen, warum das Mitmachen ein Muss ist. Dann klappt’s einfach besser mit der Abwehr.