Absicherung in allen Bereichen - dank psychologischer Aspekte

Schulungen und Präventionsmassnahmen im Bereich der Arbeitssicherheit gehören heutzutage zum Standard. Auch im Gesundheitswesen ist nur allzu gut bekannt, dass Unfälle nicht nur finanzielle Folgen nach sich ziehen können. Doch die Arbeitssicherheit beschränkt sich nicht nur auf den analogen Bereich, auch digital lauern Gefahren, die sich mit den richtigen Präventionsmassnahmen verhindern lassen. Wie also kann man sich im Netz, genauso schützen wie im Arbeitsalltag vor Ort? «Awareness» bietet hier, unter Einbezug psychologischer Aspekte, eine erfolgversprechende Antwort, die ich als Awareness-Experte im Rahmen einer Bachelorthesis näher untersucht habe.

MELANI, die Melde- und Analysestelle Informationssicherung des Schweizerischen Bundesrats, zählt Spitäler längst zur kritischen Informatik-Infrastruktur. Zu Recht, wie die immer häufiger vorkommenden Übergriffe beweisen. In den letzten Jahren wurden teils schwerwiegende Cyberangriffe auf Schweizer Gesundheitsinstitutionen zunehmend publik, bis 2020 dann der erste Angriff mit Todesfolge dazu kam. Fakt ist, es kann jeden treffen und das Gesundheitswesen ist für Cyberkriminelle ein besonders attraktives Ziel. Und dazu zählen kleine Privatpraxen genauso wie grosse Institutionen. Aber das war nicht immer so, oder?

Arbeitsausfälle - digital genauso wie analog

Wer die Schuld dieser auftretenden Gefahren bei der Digitalisierung sucht, vergisst, dass Unfälle und Gefahren auch im analogen Bereich lauern. Tatsächlich liess sich in Unternehmen eine Verbindung mit Arbeitsunfällen und niedriger Awareness, wie die Achtsamkeit im Umgang mit IT-Sicherheit genannt wird, feststellen. Nur ist im Bereich der Cybergefahren, der Leidtragende nicht direkt der Unfallverursacher, sondern die/der Patient/-in beziehungsweise ihre/seine schützenswerten Daten oder sogar ihre/seine Gesundheit. Denn Cyberangriffe haben auch zur Folge, dass beispielsweise Beatmungsgeräte oder andere medizinaltechnische Geräte vom Netzwerk getrennt werden müssen. Sogar die Übernahme deren durch Cyberkriminelle ist schlimmstenfalls möglich. Zudem bedeutet ein Arbeitsunfall oft den Ausfall des Opfers, während ein Cyberangriff den kompletten Betrieb lahmlegen kann. Es macht also Sinn, neben der elementaren Arbeitssicherheit, genauso Wert auf eine adäquate Schulung im Bereich der Awareness zu legen. Was genau aber kann geschult werden, um die IT-Sicherheit im Unternehmen zu steigern?

Drei der Faktoren, die eine wesentliche Rolle spielen

Persönliches Wissen, Einstellung und Verhalten zur IT-Sicherheit haben einen signifikanten Einfluss auf die Awareness. Unter anderem zählt dazu, als wie bedeutend der Mitarbeitende die getroffenen Sicherheitsmassnahmen wahrnimmt und noch viel wichtiger, als wie verbindlich er die Einhaltung deren empfindet. Dies kann mit gewissen Persönlichkeitsfaktoren, wie beispielsweise der Arbeitsvermeidung, Gewissenhaftigkeit und Risikobereitschaft je nach Ausprägung positive oder negative Zusammenhänge aufweisen. In meiner Arbeit hat sich das Wissen als grösster Faktor zur Verbesserung der Awareness dargestellt. Ist also beispielsweise eine Gesundheitsfachperson darauf geschult worden, wird sie ein virenbelastetes, als harmlos getarntes E-Mail vor dem Öffnen eher prüfen und kann so eine Attacke verhindern. Wissen schützt also auch im digitalen Bereich. Diese kurze Prüfung eines Mails, kostet das geschulte Auge kaum Zeit, kann aber erheblichen Schaden verhindern. Aber wieso sollte die Gesundheitsfachperson überhaupt unvorsichtig ein Mail öffnen?

HIN

Jona Karg

Leiter Schulungswesen

Health Info Net AG
Tel. 0848 830 740
jona.karg@hin.ch
www.hin.ch

Chancen und Risiken der Persönlichkeit

Dass ein Zusammenhang zwischen den menschlichen Faktoren und der IT-Sicherheit im Gesundheitswesen besteht, wird bereits angenommen. Die Forschung in diesem Gebiet steht jedoch noch ganz am Anfang. Sie liefert allerdings bereits einige spannende Ansätze, welche die oben gestellte Frage, immerhin teilweise beantworten könnte und die ich in meiner Arbeit daher näher ergründete. Prinzipiell geht man davon aus, dass die Persönlichkeit eines Menschen genauso Einfluss auf sein Verhalten im digitalen Bereich nimmt, wie es auch in allen anderen Bereichen der Fall ist. Personen mit einer höheren Gewissenhaftigkeit tendieren dazu, sich eher an Regeln zu halten, als solche mit einer geringeren. So liess sich dies auch in Bezug auf die Arbeitssicherheit feststellen. Die gewissenhafte Gesundheitsfachperson führt also die vorgeschriebenen Präventionsmassnahmen zur Arbeitssicherheit auch dann aus, wenn sie unbeobachtet ist.
Eher negative Auswirkungen lassen sich dabei wiederum in Zusammenhang einer erhöhten Risikobereitschaft feststellen. Tendenziell lässt sich eine hohe Risikobereitschaft auf riskante Hobbys projizieren, es wäre aber falsch zu glauben, dass alle Mitarbeitenden mit waghalsigen Hobbys generell eine Gefahr für die IT-Sicherheit darstellen. Aber welche Faktoren bieten nun am meisten Potential?

Faktor Mensch x Faktor Wissen

Die Faktoren Einstellung und Verhalten hängen also unter anderem auch mit der Persönlichkeit des Menschen als Individuum zusammen. Der Faktor Wissen hingegen, kann durch äussere Einflüsse gesteuert werden und bietet das grösste Potential. So kann die Awareness durch das Vermitteln von vertieftem Wissen durch Schulungen vor Ort oder digitale Lernportale massiv gesteigert werden. Ähnlich wie bei der Unfallprävention: Kennt man die Stelle am Boden, auf der immer alle ausrutschen, können die internen Prozesse so angepasst werden, dass der Unfall-Hotspot behoben werden kann.
So zeigen Awareness-Kampagnen genau auf, wo die Gefahren lauern und liefern dann entsprechende Präventiv-Massnahmen. Wobei nicht nur das Verhindern von Cyberattacken im Fokus steht, sondern auch das korrekte Handeln, sollte es trotz aller Vorsicht zu einem Übergriff kommen. Aber wie bleibt man ständig aware?

Unfallfrei auch im Netz - Awareness nach Mass

Wirklich erfolgreich, ist man in Bezug auf Mitarbeitende, die ständig aware bleiben, aber nur durch stetige Sensibilisierung. Dazu gehören nicht nur Schulungen und interaktive Lernportale, sondern auch das Auseinandersetzen mit aktuellen Themen zur Informationssicherheit. Das ist mit ein Grund, warum ich aktuelle Beiträge zu diesen Themen im HIN Blog für alle zugänglich mache. Denn nur ständige Awareness und stetige Neugierde macht den Faktor Mensch zur echten Chance im Bereich der Informations- genauso wie der Arbeitssicherheit.

So bleiben Sie und Ihr Team aware und vor allem unfallfrei – hoffentlich in allen Bereichen.

Speziell auf Gesundheitsinstitutionen zugeschnittene Schulungen sowie ein auf psychologische Faktoren ausgerichtetes Awareness Portal für interaktives E-Learning finden Sie unter www.hin.ch/hinacademy/

Quellenverzeichnis

1. Artikel zu Cyberattacken im Gesundheitswesen «Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf» URL: https://www.handelsblatt.com/technik/sicherheit-im-netz/cyberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html?ticket=ST-717233-INW7HXxoxzxSj76hsHQ9-ap4, 18.09.2020

2. Bachelor Arbeit «Faktor Mensch in der Cybersecurity – eine psychologische Untersuchung der Information Security Awareness von Gesundheitsfachpersonen» von Jona S. Karg, Mai 2020,

Zürcher Hochschule für Angewandte Wissenschaften, Studiengang Angewandte Psychologie