audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Security Awareness

Zusammenfassung

Unternehmen sind seit Anbeginn des Informationszeitalters Cyber-Gefährdungen ausgesetzt, doch wird dabei ein wichtiger Fakt von Unternehmen häufig außer Acht gelassen: Cyber-Gefährdungen erfordern in über 99 % aller Attacken eine menschliche Interaktion[1]. Dennoch sind IT-Sicherheitsmaßnahmen, die von Unternehmen etabliert werden, sehr häufig ausschließlich technischer Natur. Weiter noch, herrscht häufig die Meinung IT-Sicherheit, oder um den Begriff auf sämtliche Werte (engl. Assets) eines Unternehmens zu erweitern, Informationssicherheit sei nur kostspielig, brächte keinen erkennbaren Mehrwert und würde sowieso niemals benutzt. Das Ziel zu erreichen, dass eine Sicherheitsmaßnahme niemals benötigt wird ist dabei allerdings eher positiv als negativ zu sehen, denn eine Brandmeldeanlage oder Airbags im Auto hoffen wir auch niemals benutzen zu müssen.

Problemstellung

Wie sollten Unternehmen also der Diskrepanz zwischen dem Gefährdungsfeld und der bisherigen, eher technischen, Herangehensweise begegnen? IT-Sicherheit und Datenschutz werden von Menschen und damit sowohl von Geschäftsführungen, Manager*innen, Mitarbeiter*innen sämtlicher Unternehmen im Alltag als belästigend, aufwändig und sogar einschränkende Themen angesehen. Diese Tatsache rührt häufig daher, dass digitale Gefährdungen zumeist nicht greifbar oder verständlich sind. Menschen verstehen Daten und Informationen zumeist noch nicht als Werte, weder privat noch dienstlich. In der sich rasant verändernden digitalen Welt fällt es den meisten Menschen schwer den Überblick zu behalten bei den Fragestellungen: Was ist schutzwürdig und was ist vertrauenswürdig? Unsere Smartphones[2] sind mindestens genauso schutzwürdig sind wie ein physischer Schlüsselbund. Zugänge zu digitalen Plattformen sind viel schutzwürdiger als z.B. eine EC-Karte, denn bei letzterem herrscht zumindest ein Zahlungslimit. Dennoch sind 7 der 10 häufigsten Kennwörter aus dem Jahr 2019 triviale Zahlenfolgen[3]. Man könnte daraus schließen, dass es den Menschen egal ist, was mit Ihren Daten und Informationen, privat oder dienstlich geschieht. Unserer Erfahrung nach entspricht dies jedoch nicht der Realität. Die Realität ist, dass die meisten Menschen nicht sensibel sind für Cyber-Gefährdungen. Drei zentrale Fragen stellen die Menschen, mit denen wir arbeiten dabei immer wieder: Was existieren für Gefährdungen? Was kann mir und meinem Unternehmen geschehen? Wie erkenne ich Gefährdungen? Wichtig zu verstehen ist: Nicht jeder muss Security-Experte sein, denn im Brandschutz ist auch nicht jeder Feuerwehrfrau oder Feuerwehrmann. Dennoch sollte jeder einige Grundregeln verinnerlichen.

Bedrohungen und Abhilfe

Die häufigste Bedrohung für Unternehmen herrscht häufig darin, dass sogar Führungspersönlichkeiten von Unternehmen keine Sensibilität (engl. Security Awareness) besitzen. Dabei nimmt die Bedrohungslage von Tag zu Tag zu[4] und Unternehmen täten gut daran, eine Sicherheitskultur in Ihren Reihen zu etablieren.

Dies sollte immer mit der strategischen Ausrichtung des Unternehmens im Bereich Sicherheit beginnen. Die folgende Checklist hilft dabei, zu identifizieren, wie Ihr Unternehmen sicherheitstechnisch aufgestellt ist:

1. **Kritikalität feststellen:** Hängen unternehmenswichtige Prozesse an IT-Systemen?

[1] https://www.proofpoint.com/us/resources/threat-reports/human-factor.
[2] Und sämtliche weitere IT-Geräte. Smartphones sind hier nur exemplarisch genannt.
[3] https://de.wikipedia.org/wiki/Listen_der_häufigsten_Passwörter.
[4] https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.

2. **Management Commitment:** Steht die Geschäftsführung hinter dem Thema Sicherheit oder ist die IT-Abteilung „Einzelkämpfer“?
3. **Bisherige Sicherheitsvorfälle überprüfen:** Welche Sicherheitsvorfälle (Verletzungen von Vertraulichkeit, Integrität oder Verfügbarkeit von Assets) wurden im letzten Jahr erkannt und behoben? Ein Richtwert dabei ist: Sind keine Sicherheitsvorfälle durch Mitarbeiter*innen gemeldet worden, ist die Security Awareness im Unternehmen höchstwahrscheinlich sehr niedrig, denn Vorfälle geschehen regelmäßig.
4. **Niveau ermitteln:** Führen Sie Messungen (Umfragen, Tests, etc.) durch, die ein Niveau der Security Awareness hervorbringen.

Besonders aus den Messungen lassen sich dabei eklatante Schwächen in gewissen Bereichen identifizieren und nur wer Schwächen identifiziert kann diese auch beheben. Trainieren Sie Ihre Kolleg*innen zu möglich auftretenden Angriffen. Konzentrieren Sie sich dabei unbedingt auf alle möglichen Kommunikationskanäle (E-Mail, Telefon, Chat, Instant Messaging, etc.). Training kann auf unterschiedliche Arten geschehen und sollte so gewählt sein, dass die Trainingsform möglichst nah an der Realität liegt.

Der wichtigste Punkt jedoch: Schaffen Sie eine Kultur, in der Mitarbeiter*innen einander helfen, die wichtigsten Sicherheitsregeln Ihres Unternehmens umzusetzen. Ermutigen Sie sie auch, diese Regeln auch im privaten Bereich anzuwenden und zu üben. Erlauben Sie Fehler auch im Security Bereich und verbessern Sie ihr Unternehmen du gesteigerte Aufmerksamkeit und Bewusstsein nachhaltig. Transparenz und Information sind dabei wichtige Faktoren, wenn Menschen den Sinn und Zweck hinter Maßnahmen verstehen, wenden sie diese besser und häufiger an. Passen Sie auf sich, Ihre Daten und die Daten Ihrer Kolleg*innen auf.

Autor und Ansprechpartner

Sascha Knicker
Senior Consultant Datenschutz und Informationssicherheit

Schwerpunkte: Datenschutz, TISAX, ISO 27001

Mail: s.knicker@audatis.de
Fon: 05221 87292-07

LinkedIn | Twitter | XING

Haben Sie noch Fragen?

Wir haben versucht, alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Wir unterstützen Sie gerne bei der Planung von datenschutzkonformen und sicheren Apps und der Beantwortung aller Fragen in Bezug auf die pragmatische Umsetzung des Datenschutzes und der Informationssicherheit.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de