Sicherheit lohnt sich

Informationssicherheit in Zeit von Corona

Inhaltsverzeichnis

Vorbemerkung

Will man ein Ziel erreichen, ist es am besten: Augen zu und einfach durch. Trotz Sicherheitswarnung einfach weiter. Es wird schon gutgehen.

Wir stehen oft vor der Wahl, nein, eigentlich ist es ein Dilemma: Auf der sicheren Seite bleiben und nichts erreichen oder die Sicherheitswarnung ignorieren und weitermachen – auf die Gefahr hin, auf eine digitale Mine zu treten.
Sicherheitsrelevantes Verhalten ist von vielen Faktoren abhängig. Zum Beispiel auch davon, welcher Vorgesetzte gerade in der Nähe ist: Ist es der Sicherheitsbeauftragte des Unternehmens, für den Sicherheit der Lebenszweck ist - oder der Abteilungsleiter, der dringend auf Informationen wartet. Wie auch immer man entscheidet: Jedes Verhalten hat Folgen – und seinen Preis.

Informationssicherheit ist generell komplex, vielschichtig und abstrakt. Informationssicherheit ist schwer zu greifen und von situationsbedingten Prioritäten abhängig. Für den Menschen vor dem Rechner ist es ein (Arbeits-) Leben, das von Möglichkeiten, Wahrscheinlichkeiten, sich ständig ändernden Verantwortlichkeiten und konfligierenden Erwartungen geprägt ist.

Die Frage ist: Wie macht man es richtig machen, damit es nicht falsch ist?

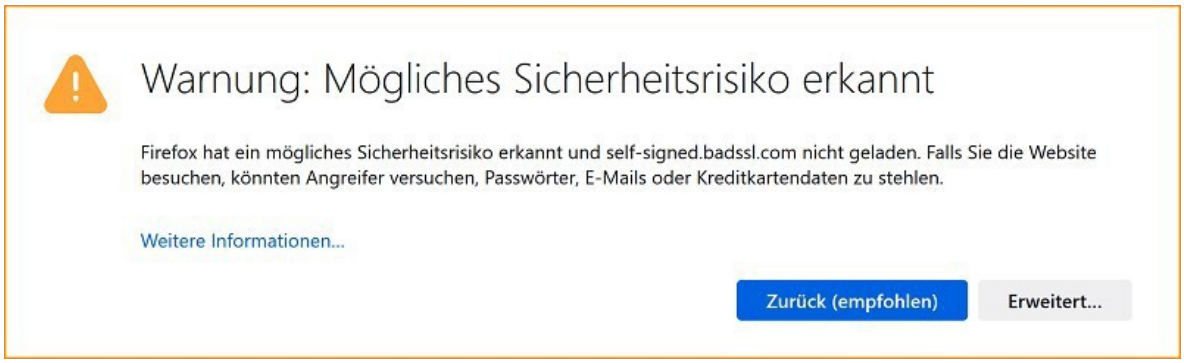
1 Sind Ausgaben für Sicherheit (betriebswirtschaftlich) sinnvoll?

Für Sicherheitsexperten ist es keine Frage: Sicherheit ist wichtig. Überlebenswichtig. Privat wie beruflich, für eine Person genauso wie für einen Betrieb.

So denken wir CISOs, Auditoren oder Sicherheitsberater. Doch jeder, der versucht hat, einer Marketing-Abteilung die iPhones wegzunehmen oder einen Geschäftsführer davon zu überzeugen, dass es keine gute Idee ist, das Passwort an die Assistenz weiterzugeben, der weiß: das ist nicht einfach. Offensichtlich gibt es Dinge, die wichtiger sind als „Sicherheit" - im Privatleben genauso wie im Geschäftsleben.

1.1 Ziele, Verantwortlichkeiten und Erwartungshaltungen in kritischen Situationen

Folgende Situation: ein Mitarbeiter/ein Benutzer bekommt eine Zertifikatswarnung, die ihm sagt, dass er eine Website nicht besuchen soll. Der Mitarbeiter kennt die Regeln, er sieht die Warnungen in seinem Browser, aber er muss – so meint er – unbedingt dorthin, weil er die Information, die er jetzt gerade braucht, nur dort bekommt. Was soll er tun? Was wird er tun?



Hat der Mitarbeiter in diesem Moment den *CISO (**c**hief **i**nformation **s**ecurity **o**fficer)* neben sich, wird er mit dem Versuch, die Warnung wegzuklicken, nicht weit kommen. Der CISO zieht das Netzkabel schneller als der Mitarbeiter die Sicherheitsausnahme bestätigen kann. Es ist nichts passiert, aber auch das ursprüngliche Ziel des Mitarbeiters ist nicht erreicht.

Hat der Mitarbeiter in diesem Moment jedoch seinen *Abteilungsleiter* neben sich, der mit allen Anzeichen von Nervosität auf diese letzte Information von genau dieser Website wartet, wird er, der Mitarbeiter, die Sicherheitsausnahme schneller bestätigen als ihm die Regelverletzung in den Sinn kommt. Das Ziel ist erreicht, passiert ist auch nichts.

*Im **ersten Fall*** (die Website nicht aufrufen) hat sich der Mitarbeiter regelkonform verhalten, macht sich aber berechtigte Sorgen, weil er seinen Arbeitsauftrag nicht erledigt hat.

*Im **zweiten Fall*** (die Website aufrufen) hat sich der Mitarbeiter sorglos verhalten und muss sich deswegen entsprechend keine Sorgen machen. Er hat seinen Auftrag ja erledigt.

*In **beiden Fällen*** zahlt der Mitarbeiter aber einen Preis. *Im ersten Fall* zahlt er den Preis der – möglicherweise erfolglosen – Rechtfertigung seiner Entscheidung, seinen Beitrag zum Unternehmenserfolg aus Sicherheitsgründen nicht geleistet zu haben. *Im zweiten Fall* zahlt er den Preis, das Risiko eines *Man-in-the-Middle-Angriffs* (MITM) akzeptiert zu haben („Risiko akzeptieren und fortfahren").

Sicherheit hat also ihren Preis. *Hält* sich der Mitarbeiter an die Regel, zeigt er damit, dass ihm die Befolgung von Regeln wichtiger ist als der Abteilungsleiter und der Erfolg der Abteilung. Das hat zukünftige persönliche Konsequenzen. Hält sich der Mitarbeiter aber *nicht* an die Regel, gibt es keine zukünftigen persönlichen Konsequenzen. Erstens sind

MITM-Angriffe eine bedrohte Spezies. SSL-Zertifikate sind bei Websites inzwischen endemisch. Und – zweitens – selbst wenn der Rechner des Mitarbeiters kompromittiert wird: die Rechnung zahlt das Unternehmen. Aus der Sicht des Mitarbeiters ist das eine Externalität, ein negativer externer Effekt, der für das eigene Verhalten keine Rolle spielt.

In der Gedankenwelt des *Homo Ökonomikus* unserer modernen Marktwirtschaft ist es vollkommen rational, auf den Vorteil der Ich-AG zu achten und alles andere dem „Markt" zu überlassen.

1.2 *Informationssicherheit: vielschichtig, komplex, abstrakt*

Informationssicherheit ist ein abstraktes, vielschichtiges Konzept, das ein Verständnis komplexer Wirkzusammenhänge voraussetzt. Entscheidet man sich dafür, den Ratschlägen, Vorgaben und Pflichten für informationssicheres Handeln Folge zu leisten, ist das immer mit Nachteilen und Unbequemlichkeiten verbunden. Informationssicherheit kostet Geld, Zeit und Aufwand für die Änderung oder Erweiterung bequemer und gewohnter Vorgehensweisen - und am Ende hat man die Erwartungen von Abhängigen, Vorgesetzten und Partnern enttäuscht.

Und die Belohnung dafür? Die Belohnung dafür ist, dass die *Wahrscheinlichkeit*, dass etwas Schlimmes passiert, *weniger groß ist*. Wenn wegen unsicherer Handlungen etwas Schlimmes passiert, dann kann das Tage, Wochen oder Monate von der – im Sinne der Informationssicherheit – falschen Entscheidung entfernt sein und die Folgen sind zu einem erheblichem Teil Externalitäten, die von anderen getragen oder zumindest mitgetragen werden.

Der Gedanke drängt sich auf, dass wir es bei „Sicherheit im Cyberspace" mit einer Situation zu tun haben, die uns inzwischen aus der Entwicklung der Corona-Pandemie oder der Klimakrise und dem Umgang damit wohl bekannt ist.

Und es ist klar, dass es nicht leicht ist, einen Unternehmensleiter oder einen Behördenleiter davon zu überzeugen, dass es eine gute Sache ist, aus freien Stücken im Hier und Jetzt Nachteile für die mögliche Reduzierung einer Schadensmöglichkeit in der Zukunft auf sich zu nehmen.

1.2.1 *„Pay me now - or pay me later"*

Eine oft gebrauchte Metapher, die eigene Aufwände für Bemühungen um Sicherheit im Cyberspace im gewohnten Narrativ des „rational agierenden Marktteilnehmers" zu platzieren und als notwendig und nützlich erscheinen zu lassen, ist die Feststellung:

„Aufwände für Informationssicherheit sind Betriebskosten".

Ein Werbespot für Fram Ölfilter aus dem Jahr 1972 veranschaulicht das Argument unübertroffen klar und einprägsam in folgender Szene:

Ein Automechaniker rollt auf seinem Liegebrett unter einem Automobil hervor. In einer Hand hält er einen Kolben mit verschlissenen Kolbenringen, in der anderen Hand einen Ölfilter. Der Mechaniker schaut von einer Hand zur anderen und sagt: *„You can pay me now, or you can pay me later."*

Hier die Analogie: es ist, wie es ist. Reibung ist Teil des Automotors. Maßnahmen zur Verminderung von Reibung sind Betriebskosten, die dem Fahrzeugführer entstehen. Sie sind unvermeidbar. Man muss zahlen. Wie man zahlt, ist die einzige Wahl, die man hat. Man kann regelmäßig den Öl- und Ölfilterwechsel bezahlen - oder die Zerstörung, die irgendwann ein Kolbenfresser im Motor anrichtet.

Mit der Informationssicherheit ist es nicht anders. Die Aufwände für Informationssicherheit sind Betriebskosten. Sie sind unvermeidbar. Man muss zahlen. *Wie man zahlt, ist die einzige Wahl, die man hat.* Man kann ein Budget für Informationssicherheit einrichten und die Betriebskosten zahlen, wie das Unternehmen auch mit anderen regelmäßig und dauer-

haft auftretenden betrieblichen Aufwendungen umgeht. Oder aber: man tut nichts (oder zu wenig) und zahlt dann zu einem unvorhersagbaren Zeitpunkt eine nicht vorhersagbare Summe, wenn die Katastrophe da ist.

1.2.2 *Argumente? Legitimations-Erzählungen.*

Ja, wir kennen die „Argumente“: Das ist der Kolben eines amerikanischen Autos, kein Mercedes oder BMW. Wir hören von einer Tante, die mit ihrem 500 SEL fast 800.000 Kilometer gefahren ist, ohne das Öl zu wechseln und erst recht nicht den Ölfilter. Vielleicht kommt man damit durch. Vielleicht hat man Glück. Für die meisten, die weniger Glück haben, ist es aber eine gute Strategie, sich nicht darauf zu verlassen, dass man dem Kolbenfresser durch Glück entgeht. Für die meisten ist der regelmäßige Wechsel von Öl und Ölfilter eine gute Idee.

Mit der Informationssicherheit einer Organisation ist es nicht anders. Eine Abteilung kann ohne ausreichende Sicherheitsvorsorge davonkommen. Aber über alle Abteilungen hinweg ist mangelnde Sicherheitsvorsorge einfach leichtsinnig und riskiert den Bestand der Organisation.

Der Mechaniker im Fram-Werbespot ist in der Rolle des freundlichen Beraters. Er sagt nur, was passieren kann und was über kurz oder lang den meisten widerfahren *wird*, die sich nicht darum kümmern, wie man die Gesundheit des Motors erhalten kann.

Der Informationssicherheitsbeauftragte hat in der Organisation die gleiche Rolle. Er sagt, was passieren *kann* und was irgendwann in der Zukunft passieren *wird*, wenn man sich nicht darum kümmert, die Sicherheit der Organisation auf dem notwendigen Niveau zu halten.

2 Wieviel Sicherheit braucht man?

CISOs sprechen mit Inhabern, Leitern und Managern von Organisationen. Die wichtigste Aufgabe des Managements ist es, die (Vermögens-) Werte und Interessen ihrer Organisation zu schützen. Sicherheit ist ein Mittel zu diesem Ziel. Sicherheit hat ihren Preis und jeder Manager wird wissen wollen, was das aktuell notwendige Sicherheitsniveau ist, das erreicht werden muss und was das kostet.

Sicherheitsmaßnahmen müssen in den Augen der Manager *effizient* sein. Eine Sicherheitsmaßnahme ist effizient, wenn sie das Sicherheitsziel mit geringerem Aufwand erreicht als alternative Maßnahmen, wobei die Alternative „keine Sicherheitsmaßnahme“ immer auch mit betrachtet werden muss.

2.1 Sicherheitsniveaus? Wie hoch ist hoch genug?

Bruce Schneier hat vor fast 20 Jahren – auf der BlackHat Konferenz im Juli 2003 – die Tatsache festgestellt, dass bei Sicherheitsentscheidungen viele Erwägungen eine Rolle spielen und beiläufig definiert, was das „notwendige Sicherheitsniveau“ einer effizienten Organisation ist.

Das Niveau der Informationssicherheit einer Organisation ist hoch genug, wenn die Sicherheitsvorkehrungen zum Schutz der Ressourcen der Organisation *so gut sind*, dass Bedrohungen (roter Pfeil) die Ressourcen nicht erreichen können, sondern abgewehrt werden (grüner Pfeil). Abwehr von Gefahren bedeutet in diesem Modell, dass die Aufwände für den Angreifer so hoch sind, dass er sich lieber eine andere Zielorganisation sucht, die ihre Ressourcen nicht so gut geschützt hat.

2.2 Auch die Angreifer müssen kalkulieren

Der Angreifer wird in diesem Modell als rational agierender Marktteilnehmer gesehen. Er ist ein Produzent von Bedrohungen, die in der Lage sind, Ressourcen von anderen Marktteilnehmern zu monetarisieren. Wenn die Aufwände für die Herstellung, Ausführung und erfolgreiche Monetarisierung der Bedrohung höher werden als die erwartbare

Monetarisierung des Erfolgs, dann wird der Angriff sinnlos und die Bedrohung wird auf ein leichter erreichbares Ziel gerichtet.

Das Denkmodell von Bruce Schneier ist heute noch attraktiver als vor 20 Jahren. Die Bedrohungen werden inzwischen ja wirklich von gut organisierter Cyberkriminalität (dazu gehören auch staatliche Akteure und konkurrierende Marktteilnehmer) produziert und orchestriert. Script-Kiddies, die Angriffe starten, weil es geht, weil es Spaß macht oder weil sie einen nicht mögen, das ist nicht mehr das Problem, mit dem Organisationen heute zu kämpfen haben.

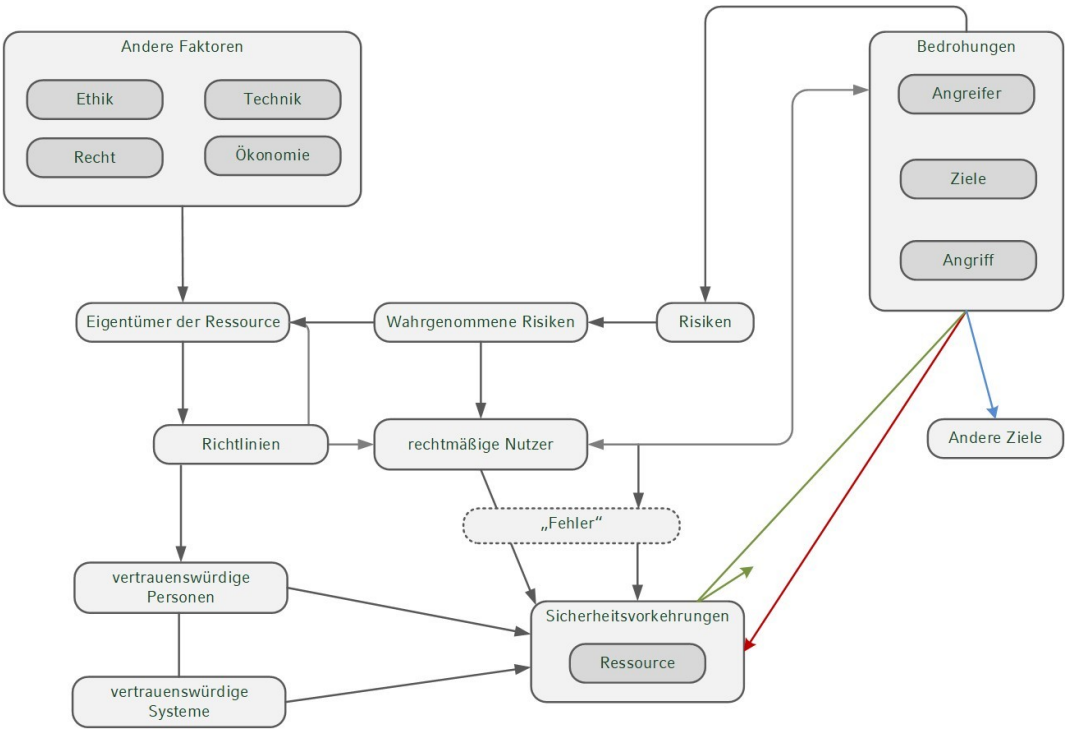
Das Modell nimmt auch den Argumenten die Kraft, die sagen, dass ein Angreifer mit genügend Aufwand immer erfolgreich sein wird – und man deswegen eh nichts machen kann und machen muss. Ein rational agierender Angreifer erbringt nur den Aufwand der sich für die erwartete Monetarsierung des Angriffserfolgs lohnt. Wird der Aufwand zu hoch, lässt er vom Angriff ab. Für *dieses* Mal.

Sicherheitsvorkehrungen müssen in diesem Modell nicht perfekt sein, sondern nur „gut genug" … und das kann man so gut wie immer schaffen.

Das Modell gibt auch Hinweise darauf, wie sich Sicherheitsvorkehrungen in Organisationen entwickeln. Ethische Erwägungen, technische Möglichkeiten, Konsequenzen von Rechtsverletzungen (z.B. Datenschutz), Wirtschaftlichkeitserwartungen und vieles mehr beeinflussen die Entscheidungen derjenigen, die für den Schutz einer Ressource Verantwortung oder Teilverantwortung haben (Eigentümer der Ressource).

2.3 *Und der Markt? Und die Konkurrenz?*

Das Modell weist auch darauf hin, dass die Wahrnehmung der Risiken ein wichtiger Faktor für die Auswahl und Ausgestaltung von Schutzmaßnahmen ist. Je mehr Informationen über Absichten und Verhalten des (cyberkriminellen) Marktteilnehmers vorliegen, desto effizienter kann die Organisation handeln. Ganz normal also, Marktrationalität ist nur möglich, wenn ich den Markt kenne. Und vor allem auch das Sicherheitsverhalten der (nichtkriminellen) Mitbewerber. Der Angreifer soll ja denken, dass er seine Verdienstabsichten bei einer anderen Organisation mit ähnlichen Ressourcen mit weniger Aufwand realisieren kann.



Das Modell „marktrationale Sicherheitsaufwendungen“ hat seinen Nutzen für eine individuelle Organisation. Es erinnert uns aber auch an das Sankt-Florian-Prinzip: *„Heiliger Sankt Florian, verschon‘ mein Haus, zünd‘ and’re an!“*, laut Wikipedia eine Bezeichnung für „Verhaltensweisen, potentielle Bedrohungen oder Gefahrenlagen nicht zu lösen, sondern auf andere zu verschieben.“

Der verantwortungsbewusste CISO fragt sich, ob Sankt Florian das Grundproblem wirklich lösen kann, oder ob alles nur in einem endlosen Kreislauf mit immer mehr Sicherheitsproblemen endet.

Oder zu Lösungen ähnlich dem Emissionshandel für die Bewältigung der Klimakrise. Cyberversicherungen sind ja ein erster Schritt in diese Richtung. Je weniger Sicherheit in der Organisation, desto höher der Versicherungsbeitrag.