IT-Security zur Chefsache machen

10 Top Maßnahmen für Ihren Betrieb

Cyber Security von Anfang an
Ihr IT-Partner und Managed Security Service Provider. Seit 1994.

Thinking Objects

Das BKA[1] berichtet in seiner jährlichen Stellungnahme von einem enormen Wachstum der Cybercrime-Fälle. Mehr als doppelt so viele Straftaten als vor 5 Jahren wurden 2020 gemeldet.

Laut Bundeswirtschaftsministerium waren mindestens 50 % aller Unternehmen im vergangenen Jahr Opfer eines Cyberangriffs. Der durchschnittliche Schaden lag bei mindestens 43.700 EUR.

Diese Warnungen ließen sich schier endlos fortsetzen. Und dennoch: Dieselbe Studie kommt zum Ergebnis, dass über 50 Prozent der deutschen KMU das Risiko eines Cyberangriffs als gering einstuft.

Die Ursachen für diese Fehleinschätzung sind vielfältig:

- Risikoeinschätzung an sich ist äußerst schwierig
- anders als bspw. beim Gebäudebrand sind die Auswirkungen einer Cyberattacke nicht konkret greifbar
- Die Wirksamkeit technischer Maßnahmen wird allgemein überschätzt und vermittelt ein falsches Sicherheitsgefühl

Dabei ist es häufig gar nicht so schwer, die eigene Organisation vor erfolgreichen Attacken zu schützen. Unsere **TOP 10 Maßnahmen** helfen Ihnen dabei, die Risiken aktiv zu mindern und auch zukünftig beruhigt den Geschäftserfolg zu steuern.

1) [Bundeskriminalamt (BKA)] „Bundeslagebild Cybercrime 2020“, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html?nn=28110, 13.07.2021

Unsere TOP 10 Maßnahmen

TOP 1 Machen Sie Informationssicherheit zur Chefsache

Alles dreht sich um die Frage der Unternehmenskultur. Nicht nur im Bereich der Informationssicherheit prägen Topmanagement und Geschäftsführung die Kultur und das Klima in einem Unternehmen.

Im Englischen spricht man vom "Tone from the Top" und verbindet damit hauptsächlich Skandale, die durch Fehlverhalten oder Korruption in Führungsetagen entstanden sind. Dieses Phänomen lässt sich aber genauso gut umkehren.

Wie sollten Sie das umsetzen

Demonstrieren Sie aktiv und beständig, dass Ihnen Informationssicherheit wichtig ist. Nehmen Sie ihre aufgestellten Regeln ernst und leben Sie das vor. Zeigen Sie Interesse für das Thema und lassen Sie sich dazu von Ihren Experten oder Dienstleistern beraten. Lassen Sie sich die größten Risiken aufzeigen und bewerten Sie diese.

Prüffragen zur Umsetzung:

- Halte ich mich an Regeln?
- Fordere ich sicheren Umgang mit IT ein und lebe ich das vor?
- Lasse ich mir zu IT-Risiken berichten?
- Kann ich die größten Risiken benennen?
- Kenne ich meine "Schmerzgrenze", die meinen Risikoappetit bestimmt?

TOP 2 Identifizieren Sie Ihre Kronjuwelen - diese sollten sie schützen

Alles mit voller Kraft zu schützen wird nicht nur fehlschlagen, es wird auch Unsummen an Kosten verursachen. Daher ist es nicht zielführend alles gleichermaßen zu schützen.

Es sollten dort Maßnahmen ergriffen werden, wo die Zukunft eines Unternehmens existenziell gefährdet werden kann.

Wie sollten Sie das umsetzen

Um die Kronjuwelen zu identifizieren, sollten sie zu bewährten Methoden greifen. Das ist oft nicht ganz trivial, denn häufig gibt es für Ihre Organisation oder Unternehmung nicht "das Cola-Rezept".

Zu empfehlen sind zwei Methoden:

1. Skizzieren Sie Ihre Wertschöpfungskette. Stellen Sie sich die Frage, welche Abschnitte von IT abhängig sind und welche Abschnitte auch ohne IT umgesetzt werden könnten.
2. Führen Sie eine Prä-Mortem Analyse durch.

Eine Prä-Mortem Analyse funktioniert so:

Sie stellen folgende Hypothese auf:

> Aufgrund einer erfolgreichen Cyberattacke ist meine Unternehmung in 6 Monaten insolvent.

Dann erstellen Sie in einem Gedankenspiel die Herleitung: Was ist passiert? Welche Menschen, Systeme und Prozesse waren maßgeblich beteiligt? Wie kann dieses Szenario effektiv verhindert werden?

Prüffragen zur Umsetzung:

- Kennen Sie ihre "Kronjuwelen"?
- Wissen Sie, was es zu schützen gilt?
- Was macht Ihre Unternehmung am Markt erfolgreich?
- Welche Art von Vorfall oder Angriff würde ihre Organisation empfindlich verletzen?

TOP 3 Planen Sie den Notfall

Als Dienstleister im Bereich IT-Security und Teilnehmer an der Cyberwehr BW werden wir häufig zu Vorfällen hinzugezogen, wenn es schon zu spät ist.

Das Bild ist häufig ähnlich: Die gesamte Firma verhält sich wie ein Haufen kopfloser und aufgescheuchter Hühner. Die Kollegen nennen das: "Headless Chicken Mode". Dieser Zustand ist im Falle einer akuten Krise äußerst kontraproduktiv. Besser ist es, wenn alle Beteiligten wissen, wie zu reagieren ist und was auf sie zukommt.

Wie sollten Sie das umsetzen

Planen Sie für den Notfall. Da IT-Notfälle immer eher abstrakt wirken, sollten sie zur Notfallplanung folgendes Szenario anwenden:

- Der Hauptstandort Ihrer Organisation ist unbenutzbar (egal ob Pandemie, Meteorit oder Cybervorfall)

Legen Sie fest, wer welche Aufgaben übernehmen muss. Erstellen Sie Kommunikationspläne: Wer berichtet in welcher Frequenz an wen. Erstellen Sie einen groben Ablaufplan und testen Sie diesen.

Nichts ist schlimmer als ein IT-Mitarbeiter, der unter großem Stress und Druck versucht so schnell wie möglich die Systeme wiederherzustellen und ein Geschäftsführer, der an diesem Schreibtisch alle 5 Minuten nachfragt, wie lange das wohl noch dauern wird….

Lassen Sie sich die größten Risiken aufzeigen und bewerten Sie diese.

Prüffragen zur Umsetzung:

- Wissen alle wichtigen Personen was im Notfall zu tun ist?
- Wissen Sie, wen Sie im Notfall womit beauftragen müssen?
- Wer berichtet im Notfall an Sie? Und wie oft?

TOP 4 Patchen Sie alle Systeme regelmäßig

Patchen ist der Fachbegriff für die Installation von Sicherheitsupdates. Software ist komplex und fehlerhaft. Solche Fehler in Software führen zu Schwachstellen und Sicherheitslücken. Diese werden durch Angreifer ausgenutzt.

Nahezu alle breit angelegten und erfolgreichen Angriffswellen der vergangenen Jahre sind auf Schwachstellen in Software zurückzuführen:

- Wannacry (2017)

Prüffragen zur Umsetzung:

- Sind für alle Systeme und Softwarekomponenten die automatischen Updates aktiviert?
- Ist überflüssige Software deinstalliert?

- Sandworm (2018)
- Emotet (ab 2019)
- Hafnium (2021)

In allen Fällen gab es zum Zeitpunkt breit angelegter Angriffe bereits wirksame Schutzmaßnahmen: Sicherheitsupdates.

Wie sollten Sie das umsetzen

Die notwendigen Maßnahmen sind zwar technisch, können jedoch von ihrer IT, ihrem Dienstleister oder Ihnen persönlich leicht angewandt werden.

Stellen Sie sicher, dass alle Software und Betriebssysteme immer zeitnah mit allen verfügbaren Updates versorgt werden. Aktivieren Sie dazu immer die automatische Update-Funktion.

Verzichten Sie außerdem auf Software, die sie nicht benötigen und deinstallieren Sie diese.

Wenn Updates nicht möglich sind, weil es sich zum Beispiel um einen Computer zur Maschinensteuerung handelt, dann trennen Sie das System vom Internet.

TOP 5 Schulen Sie Ihre Mitarbeiter

Prüffragen zur Umsetzung:

- Wissen Ihre KollegInnen, an wen sie sich im Fall eines Cyberangriffs wenden sollen?
- Ist klar, welche Schritte notwendig sind, um Cyberangriffe einzudämmen?

Oben hatten wir es bereits vom "Headless Chicken Mode". Stellen Sie sich dieses Bild bei einem Gebäudebrand vor: Alle rennen wild umher, manche versuchen mit Wasser zu löschen, andere mit Schaum oder Pulver. Wieder andere rufen Rettungskräfte, aber keiner ist auf das Wichtigste bedacht: Bei einem Brand gilt zuerst die Eigensicherung: Verlassen Sie das brennende Gebäude und helfen Sie Bedürftigen dabei. Der Brand wird von der Feuerwehr gelöscht!

Gleiches gilt im Cyber-Vorfall. Versuchen Sie nicht, Ihren Mitarbeitern die Bekämpfung von Cybercrime zu vermitteln. Dazu gibt es Experten.

Wie sollten Sie das umsetzen

Ihre Mitarbeiter und KollegInnen müssen ein paar grundlegende Dinge immer wieder parat haben und üben.

Dazu gehört das grundlegende Verständnis, dass es Cyberattacken gibt, und dass jeder Opfer werden kann. Entscheidend ist die korrekte Reaktion auf einen erfolgreichen Angriff: Meldewege müssen klar sein und erste Schritte, um sich selbst in Sicherheit zu bringen. Das kann zum Beispiel bedeuten, dass der Router vom Internet getrennt wird.

TOP 6 Klare Regeln und Prozesse – Vertrauen ist gut, Kontrolle ist besser

Prüffragen zur Umsetzung:

- Gibt es Regeln zum Umgang mit IT Systemen?
- Werden diese kontrolliert?
- Werden Verstöße sanktioniert?

Hier sei das Beispiel vom Zähneputzen bemüht: Es ist sehr einfach, den Prozess des Zähneputzens zu beschreiben. Der Prozess ist zudem leicht zu erlernen. Und dennoch: Ohne stetige wiederkehrende Kontrolle etabliert sich der Prozess nicht automatisch.

Wie sollten Sie das umsetzen

Erlassen Sie Regeln:

Was ist zum Beispiel beim Surfen erlaubt und was nicht? Worauf ist beim Umgang mit E-Mails zu achten, wieso sollte ein Schreibtisch aufgeräumt werden, etc.

Etablieren Sie Prozesse:

Wie funktioniert die Meldung eines Sicherheitsvorfalls? Wer meldet neue Risiken an die Geschäftsführung, usw.

Kontrollieren Sie diese Regeln und Prozesse und sanktionieren Sie die Missachtung. Nur so erreichen Sie das Ziel einer sicheren Organisation.

Diese Regeln und Prozesse müssen natürlich klar und verständlich formuliert, von jedem einsehbar und kommuniziert sein.

TOP 7 Sichern Sie Ihre Daten und testen Sie die Wiederherstellung

Prüffragen zur Umsetzung:

- Prüfen sie regelmäßig, ob ein Restore funktioniert?
- Haben sie die richtige Frequenz ihrer Backups festgelegt?

Böse Zungen behaupten, dass Sie gar kein Backup benötigen. Sie benötigen vielmehr die Möglichkeit im IT-Notfall ihre Daten wiederherzustellen.

Wie sollten Sie das umsetzen

Nutzen Sie für die Sicherung ihrer Daten ein Medium, welches "verschlüsselungssicher" ist. Das kann zum Beispiel ein regelmäßig gewechseltes Magnetband sein. Wichtig ist hier nicht das Medium, sondern die beiden Attribute:

- verschlüsselungssicher: Das Backup darf von einem Angreifer nicht verschlüsselt werden.
- regelmäßig: auf welchen Datenbestand können Sie verzichten? 1 Stunde? 1 Tag? 1 Monat?

Die Wiederherstellung ihrer Daten sollten sie dann natürlich immer wieder testen.

Zweimal im Jahr einen Wiederherstellungstest zu machen unterstützt zudem die Abläufe in einem echten Notfall.

TOP 8 Netzwerktrennung und Zugangskontrolle

Ein erfolgreicher Angreifer hat in der Regel dieselben Berechtigungen, die der angegriffene Anwender oder das angegriffene System hat. Als Verantwortungsträger in Ihrer Organisation haben Sie daher schon immer physische Sicherheitsmaßnahmen ergriffen: Die Personalbuchhaltung ist verschlossen, Ihr Büro wird abgeschlossen, die Eingangstüre zum Betrieb wird verschlossen, etc.

Es ist auch absolut klar, wer sich am Schreibtisch der Geschäftsführung aufhalten darf.

Diese Maßnahmen sollten sie auch in der virtuellen Welt ergreifen.

Prüffragen zur Umsetzung:

- Gibt es ein Inventar aller Netzwerkgeräte?
- Lässt sich dieses Inventar sinnvoll kategorisieren (Vertrauenswürdigkeit, Internetnutzung)?
- Ist sichergestellt, dass nur vertrauenswürdige Geräte oder Anwender Zugang zum Netzwerk bekommen?

Wie sollten Sie das umsetzen

Netzwerktrennung bedeutet, sie sollten die Organisation je nach Größe in sinnvolle Netzwerkbereiche unterteilen. So macht es häufig Sinn, einen Netzwerkbereich für bspw. die "Produktion" zu erstellen. In diesem Netzwerk befinden sich Maschinen oder Geräte, die für die Produktion (Wertschöpfung) verantwortlich sind. Diese müssen häufig nicht mit dem Internet verbunden sein. Anders ist das oft beim WLAN, denn die meisten Geräte in einem WLAN halten sich nur zum Surfen darin auf.

Bei der Zugangskontrolle stellt man durch technische Maßnahmen sicher, dass nur vertrauenswürdige oder bekannte Geräte oder Anwender mit dem Netzwerk verbunden werden. Das ist insbesondere bei Fernzugriffen (z.B. VPN) wichtig.

TOP 9 Legen Sie Wert auf sichere Passwörter

Passwörter sind der Schlüssel. Zu allem! Zu ihrem Mailpostfach, zu ihrem Unternehmen, zu Ihrer digitalen Identität!

Leider ist das problematisch, denn Passwörter sind häufig unsicher, weil sie zu kurz, bekannt oder mehrfach benutzt sind. Das gilt es zu vermeiden!

Prüffragen zur Umsetzung:

- Werden lange Passwörter erzwungen? Warum gibt es Ausnahmen?
- Ist überall, wo es möglich ist – und insbesondere bei externen Zugängen – eine Multi-Faktor-Lösung im Einsatz?
- Nutzt die Organisation die Möglichkeiten eines Passwortmanagers?

Wie sollten Sie das umsetzen

Sie sollten zunächst Wert auf zwei Dinge legen: Qualität und Einzigartigkeit. Das umzusetzen ist leicht beschrieben, leider aber nur schwer zu kontrollieren. Die Umsetzung bedeutet nach aktuellen Erkenntnissen:

- Nutzen Sie lange Passwörter - je länger, desto besser. 12 Zeichen sind Minimum. Häufig kann dies Technisch erzwungen werden.
- Verwenden Sie einzigartige Passwörter für individuelle Dienste. Das geht eigentlich nur mit Hilfsmitteln wie z.B. Passwortmanagern.
- Wenn der Zugang öffentlich ist (z.B. Remotezugang zum Unternehmen via VPN) nutzen Sie eine Multi-Faktor-Lösung (ähnlich der App zum Onlinebanking).

TOP 10 Schließen Sie eine Cyber-Risk-Police ab

Alle IT-Sicherheitsrisiken zu eliminieren würde nur gehen, wenn Sie auf IT verzichten. Das ist natürlich keine Option. Alle Risiken zu mitigieren – also zu behandeln – ist häufig mit unverhältnismäßig hohen Kosten verbunden. Es bleibt also für das Restrisiko nur die Option, das Risiko zu übertragen.

Prüffragen zur Umsetzung:

- Macht der Abschluss einer Cyberschutz-Police für meine Organisation Sinn?
- Für die Übernahme der Restrisiken in Höhe von X wäre mir eine Prämie in Höhe Y wert.

Wie sollten Sie das umsetzen

Gehen Sie auf Ihren Berater zu und informieren Sie sich. Wir als Cybersecurity Experten sind weder Versicherungsexperten noch erhalten wir Provisionen oder andere Vorteile. Allerdings stellen wir fest, dass sich der noch junge Markt der Cyberschutz-Policen rasant erweitert und nahezu alle Versicherer versuchen, ihren Marktanteil zum Zweck der Risikostreuung zu erhöhen. Das sind für Versicherungsnehmer hervorragende Bedingungen, weil die Prämien momentan verhältnismäßig niedrig sind.

FAZIT

Die Top 10 Maßnahmen aus unserer Empfehlung sind in aller Regel bereits in den meisten Organisationen vorhanden. Gleichwohl gibt es häufig Veresserungspotenziale, um die vorhandenen Maßnahmen und deren Potenziale voll auszuschöpfen. Dieses Potenzial nicht zu nutzen und deshalb auch noch Opfer einer Cyberattacke zu werden ist vermeidbar. Das ist fast so, als würde man immer ohne Gurt fahren. Es ist alles da, man muss es nur richtig nutzen!

Deshalb: Stellen Sie sich die Fragen, die wir formuliert haben. Wenn diese unklar oder nicht zufriedenstellend beantwortet werden können, dann gehen Sie auf Ihre IT Organisation oder KollegInnen zu und setzen Sie diese um!

Bleiben Sie sicher!

Thinking Objects

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

+49 711 88770400
info@to.com
www.to.com