TREX
L'EXPERT FIDUCIAIRE – DER TREUHANDEXPERTE

https://www.trex.ch

Digitalisierung

2.12.2022

Oliver Hunziker

Geschäftsführer, CIO RN IT-Unit AG, Zürich
https://rnitunit.ch

Cybersecurity – (K)ein technisches Thema!

Oliver Hunziker

«Bitte klicken Sie hier, um sofort 1 Mio $ zu erhalten …»

Sie haben sicherlich auch schon solche oder ähnliche Mails erhalten. Sind Sie darauf hereingefallen?

Vermutlich eher nicht. Zu offensichtlich ist die Verlockung, zu unglaubwürdig die Aussage.

Wie aber steht es mit Mails, die besagen, dass Ihr erwartetes Paket noch nicht ausgeliefert werden konnte, weil noch eine Gebühr aussteht, die Sie hier jetzt mit zwei Klicks unkompliziert begleichen können? Sie haben gezögert? Sie haben überlegt, ob Sie tatsächlich ein Paket erwarten?

Und hier fängt Cybersecurity an!

Aber die IT-Profis sorgen doch für meine Security?

Ja, richtig – das tun sie, oder sollten es tun. Ist Cybersecurity also ein Thema für IT-Spezialisten?

Die Antwort darauf lautet: Nein.

Natürlich ist Cybersecurity zunächst ein Themenfeld, in welchem sich hauptsächlich IT-Fachleute auskennen und bewegen. Nichtsdestotrotz ist es aber eben weit mehr als ein Spielfeld für Experten.

Eine gut aufgebaute IT-Infrastruktur ist auf sicheren Betrieb ausgelegt. Das bedeutet, dass sie möglichst redundant ist, wenig oder keine technischen Schwachstellen aufweist und weitgehend überwacht wird.

Falls Ihnen in der Aufzählung die drei Wörter «möglichst», «wenig» sowie «weitgehend» aufgefallen sind, so haben Sie gut hingeschaut. Tatsache ist, dass die gleiche Auflistung ohne diese drei einschränkenden Begriffe einfach wesentlich teurer ist.

Wie entsteht Sicherheit?

Sicherheit ist eine Mischung aus guter Planung, sauberer Wahl der eingesetzten Mittel, hohem technischem Verständnis sowie einer klugen und regelmässigen Überwachung der getroffenen Massnahmen.

Aber Sicherheit ist in erster Linie ein Gefühl, und damit etwas, das so weit von der 0/1-Welt der IT entfernt ist, wie es nur geht. Das Gefühl von Sicherheit entsteht durch die Art und Anzahl der getroffenen Massnahmen, aber eben auch, trügerischerweise, durch die Zeitdauer, in der «nichts passiert» ist.

Absolute Sicherheit kann es nicht geben. Und wie oben schon erwähnt – die Distanz zwischen der bei Ihnen eingesetzten Sicherheitslösung und der unerreichbaren absoluten Sicherheit ist tatsächlich in erster Linie eine Frage der eingesetzten Mittel, also der Kosten.

Nehmen wir als Beispiel den Vergleich mit einem Nachtwächter. Sie werden diesem Beispiel noch mehrmals begegnen.

Aus Kostengründen wird ihm die Aufgabe übertragen, die Vordertüre zu überwachen.

Die Kontrolle der Hintertür gehört daher nicht zu seinen Aufgaben.

Das ist insofern kein Problem, als die Hintertür ja geschlossen sein sollte.

Lässt nun aber jemand die Hintertür offen, waren der Einsatz des Nachtwächters und die damit verbundenen Kosten letztendlich sinnlos. Den Wächter trifft dabei keinerlei Schuld.

Level 1: Technische Sicherheit

Aus technischer Sicht, also aus dem Blickwinkel der Experten, umfasst IT-Sicherheit im Wesentlichen drei Hauptstränge.

Da ist zunächst der Aufbau der eigentlichen IT-Infrastruktur, welche so ausgelegt werden sollte, dass sie sogenannt fehlerredundant ist. Das bedeutet, dass keine unerwarteten Ausfälle passieren, dass durch solche Ausfälle keine Daten verloren gehen und dass die Kapazität der Anlage den Anforderungen genügt.

Dies geschieht durch die gezielte Auswahl von Komponenten, durch genügend Redundanz und ausreichend Reserven bei der Ressourcenplanung. Dazu gehört auch ein Sicherungskonzept, welches gegen Angriffe bestmöglich geschützt wird.

Als zweiter Hauptstrang kommt die Absicherung der Anlage dazu. Hier geht es in erster Linie darum, unbefugte Zugriffe abzuwehren, Zugänge zu sichern und die Datenintegrität zu prüfen.

Hier kommen in erster Linie Firewalls, Anti-Malware-Programme und geschützte Zugangsdaten zum Einsatz.

Der dritte Hauptstrang ist die Überwachung der Anlage und der getroffenen Sicherheitsmassnahmen.

Hier geht es darum, die Komponenten der Infrastruktur zu überwachen, um allfällige Ausfälle rechtzeitig zu bemerken und zu korrigieren, insbesondere aber natürlich um die Überwachung der Absicherung. Die Analyse und Auswertung von Rückmeldungen der verschiedenen Systeme muss regelmässig zu einer Lagebeurteilung führen. Bei Unregelmässigkeiten muss eine Intervention gewährleistet sein, ein Notfallplan sowie geeignete Abwehrmassnahmen müssen definiert und bereit sein.

Dies alles ist die weitgehend technische Aufgabe der IT-Verantwortlichen. Es setzt aber zwingend die Unterstützung des Managements voraus, da zur technischen Absicherung auch Anordnungen und Weisungen gehören, die vom Management mitgetragen und durchgesetzt werden müssen (Beispiel: Passwortsicherheit).

Wenn der Nachtwächter auf Anweisung auch verdächtige Personen einlassen muss, kann er seine Aufgabe nicht erfüllen, da ihm die Unterstützung durch den Auftraggeber fehlt.

Level 2: Der Mensch

Erinnern Sie sich an die eingangs erwähnten Beispiele von merkwürdigen Nachrichten?

Seien Sie sich stets bewusst, dass eine gute IT-Infrastruktur vermutlich bereits zahlreiche solcher Angriffsversuche abgewehrt hat. Je besser Ihre Infrastruktur ist, umso weniger solcher Attacken sollten es bis zu den Anwendern schaffen. Das bedeutet aber gleichzeitig auch, dass sie nicht vollständig ausgeschlossen sind. Cyberpiraten entwickeln ständig neue Ideen und Software, während gleichzeitig Cyberspezialisten ohne Unterlass Gegenmassnahmen entwickeln.

Die Abwehr von Angriffen ist gegenüber der Entwicklung derselben also naturgemäss immer einen Schritt im Hintertreffen.

Wie schon eingangs erwähnt – HIER fängt Cybersecurity an.

Ihre IT-Systeme können noch so ausgeklügelt sein, die grösste Schwachstelle stellt immer noch der Mensch dar. Damit sind natürlich bei Weitem nicht nur Sie und Ihre Mitarbeitenden gemeint. Auch bei der Entwicklung, der Implementierung und der Überwachung von IT-Systemen sind Menschen im Einsatz. Überall dort können Fehler passieren.

Oder etwas deutlicher: Überall dort passieren Fehler!

Was kann ich dagegen tun?

Zunächst ist es wichtig, anzuerkennen, dass die absolute Sicherheit nicht möglich ist. Dazu gehört auch, zu verstehen, dass auch die besten Schutzmassnahmen keine hundertprozentige Sicherheit garantieren können.

Daraus lässt sich dann ableiten, dass die Mitarbeitenden im Umgang mit den Gefahren geschult werden müssen, da die Gefahren real sind.

Aufmerksamkeit und Wachsamkeit im Umgang mit Daten, mit Nachrichten und mit Anfragen aller Art sollten Teil der Unternehmenskultur werden. Dinge kritisch zu hinterfragen ist in diesem Zusammenhang eine absolut positive Eigenschaft.

Die eingangs erwähnten Mailbeispiele sind relativ harmlose Versuche. Hacker und Cyberkriminelle sind heute viel weiter. Mittels Social-Engineering werden Unternehmen durchleuchtet, werden Schlüsselpersonen identifiziert und Schwachstellen ermittelt.

Ein paar Beispiele

Der sogenannte CEO-Fraud ist deshalb so bekannt, weil er schon so oft funktioniert hat. Dabei handelt es sich um Mails, die angeblich vom CEO kommen und eine Assistenzperson auffordern, eine bestimmte Summe auf ein angeblich temporäres Konto zu überweisen. Wenn man das hier so liest, fällt es einem sicherlich sofort auf, aber im Alltagsstress und unter Druck kann man sehr leicht auf eine solche Nachricht hereinfallen.

Ähnlich wie im obigen Beispiel, wo der Kriminelle sich der Reputation des CEO bedient, funktionieren auch jene Fälle, in welchen sich Anrufer als Mitarbeitende von Microsoft ausgeben, welche «kurz etwas auf Ihrem Computer überprüfen» wollen. Hier wird Microsoft als Autorität verwendet, um den Leuten das Gefühl zu geben, es sei «schon in Ordnung».

Eine andere Falle funktioniert so, dass der Mailverkehr mit einem Lieferanten abgefangen wird und plötzlich eine Antwort nicht mehr vom ursprünglichen Mailkontakt (Lieferant) stammt, sondern von Kriminellen, die sich dessen Identität bedienen. Hier werden dann oft Gründe genannt, weshalb die Zahlung für eine Bestellung nun auf ein anderes Konto gesendet werden soll.

Die Liste der Beispiele lässt sich unendlich erweitern. Dabei geht es bei Weitem nicht nur um geschäftliche Betrugsversuche. Auch die sogenannten Romance-Scams, die Nigeria-Connection und weitere Methoden des digitalen Betrugs im Privatleben gehören dazu.

Was tun?

Sensibilisieren Sie Ihre Mitarbeitenden für die Gefahr. Nehmen Sie Warnungen und Vermutungen ernst. Etablieren Sie eine Kultur, die Fehler akzeptiert, denn nur so werden Mitarbeitende ihre möglichen Fehler in diesem Bereich auch eingestehen. Und in der digitalen Welt ist Geschwindigkeit die entscheidende Komponente. Je schneller Sie und die IT-Verantwortlichen von einem möglichen Fehler erfahren, umso besser.

Veranstalten Sie regelmässige Sensibilisierungsanlässe, an welchen Ihrem Team aufgezeigt werden kann, wo die Gefahren liegen.

Stellen Sie sicher, dass Ihre IT-Infrastruktur stets aktuell und gut gesichert wird.

Bedenken Sie, dass die absolute Sicherheit nicht existiert. Zu einem guten Plan gehören also auch ausgearbeitete Szenarien, die bei einem Notfall zum Einsatz kommen.

Priorisieren Sie Ihre Daten und Anwendungen nach Wichtigkeit und Schutzbedürftigkeit. Setzen Sie Schutzmassnahmen anhand dieser Liste um.

Erarbeiten Sie einen Notfallplan und informieren Sie Ihr Team darüber, wie in einem solchen Fall vorzugehen ist.

Schliessen Sie geeignete Versicherungen ab, um im Falle eines Cyberangriffs finanziell abgesichert zu sein.

Ihre IT-Verantwortlichen oder externe Spezialisten unterstützen Sie bei diesen Massnahmen gerne.

Quellen

- Beobachter-Buch: IT-Sicherheit für KMU
- National Centre for Cybersecurity
- Fachstelle Cybercrime Kantonspolizei Zürich

Checkliste

Cybersecurity ist eine komplexe Angelegenheit, die in vielen Bereichen Aufmerksamkeit erfordert.

Vieles muss natürlich in Zusammenarbeit mit einem IT-Partner gemacht werden.

Einiges können Sie aber in Ihrem Unternehmen auch selber angehen. Dafür haben wir Ihnen die nachstehende Checkliste zusammengestellt.

Passwörter
Verwenden meine Mitarbeitenden sichere Passwörter? Wie werden diese aufbewahrt? Gibt es eine Passwortrichtlinie? Werden Passwörter mehrfach verwendet?

Zugriffsrechte
Haben die Mitarbeitenden und insbesondere die Kader nur so viel Zugriff wie nötig?
Häufig sind gerade GL-Mitglieder besonders gefährdet, weil sie hohe Zugriffsrechte haben.
Wird der Admin-Account auch für andere Dinge verwendet (Back-up, ScanToServer usw.)?
Haben die Benutzer auf ihren lokalen Geräten Admin-Rechte?

Back-up
Wie ist mein Back-up aufgebaut? Habe ich mehrere Datenstände? Sind diese extern und / oder offline verfügbar, falls ein Angriff erfolgt? Werden regelmässig Restore-Tests durchgeführt?

Datensicherheit
Sind die Daten auf den Endgeräten gelagert? Falls ja, sind diese Geräte verschlüsselt?
Dies betrifft insbesondere portable Geräte wie Laptops, Tablets usw.

Mailsicherheit
Haben wir unsere Mailsysteme geschützt? Verfügen wir über Spamfilter und Anti-Malware-Systeme?
Sind diese aktuell und verfügbar?

Sensibilisierung
Das vielleicht wichtigste Element überhaupt. Sind meine Mitarbeitenden sensibilisiert für die möglichen Gefahren und Szenarien? Werden die Mitarbeitenden regelmässig im Umgang mit möglichen Gefahren im Cybersecurity-Bereich geschult? Werden Sicherheits-Checks gemacht?

Notfallpläne
Haben wir Notfallpläne, die im Falle eines Angriffs oder eines Datenverlusts zum Einsatz kommen?
Sind diese aktuell und verfügbar?

Better safe than sorry!