01.01.2020 Qualitätssicherung

Sicherheit ist kein Projekt, das man mal vier Wochen macht

Ecclesia med GmbH

Technik ist gut und schön – solange sie funktioniert. Das gilt für die Informationstechnologie (IT) in Betrieben besonders, denn ohne IT laufen viele betriebliche Prozesse gar nicht mehr. Einen kleinen oder größeren Schaden hat fast jedes Unternehmen schon erlebt – mit unangenehmen Folgen. Wie man sich vor IT-Schäden schützt und was man ganz praktisch tun kann, erläutert Frank Rustemeyer von HiSolutions, Partner der Ecclesia Gruppe, im Interview.

Sie kümmern sich um die IT-Sicherheit von Unternehmen und Organisationen. Wie lange dauert es, einen Schaden im IT-System zu beseitigen?

Frank Rustemeyer: Das kommt auf den Schaden an. Und auf den Kunden. Manche Fälle, zum Beispiel einfache Virusattacken, können wir sehr schnell in den Griff bekommen, wenn alle Präventionsmaßnahmen stimmen. Ein gut vorbereitetes Unternehmen kann dann eine Datensicherung zurückspielen, das befallene Gerät neu aufsetzen und relativ schnell wieder im Normalbetrieb arbeiten.

Wir begleiten aber auch komplexe Schadenfälle, angefangen bei solchen, wo entweder Präventionsmaßnahmen nicht da waren oder nicht funktioniert haben, bis hin zu hochkomplexen Angriffen, die in den Bereich Industriespionage gehen, wo ganze Konzerne monatelang unterwandert werden. Da dauert es dann auch Monate, bis man solch ein Netz wieder unter der eigenen Kontrolle hat.

Das klingt teuer.

Frank Rustemeyer: Der Ausfall ist meistens das größte finanzielle Problem: Wenn beispielsweise 100 Leute nicht arbeiten können, gibt es keine Erträge, aber die Kosten laufen weiter. Dazu die Kosten, die durch den Schaden verursacht werden: Dinge, die neu installiert werden müssen, Rechtsanwaltskosten, Kommunikationskosten und Kosten für Dienstleister wie uns. Die Schadenssumme geht bei einem ernsteren Angriff sehr schnell in fünf-, sechsstellige Bereiche.

Welches sind die Hauptrisiken, denen IT-Systeme und damit die Unternehmen ausgesetzt sind?

Frank Rustemeyer: Es gibt „technisches Versagen“: Ausfälle, kaputte Datenträger, die Schäden verursachen können. Solche Risiken kann man im Betrieb recht gut einplanen und beherrschen. Schwieriger wird es in dem Bereich, wo menschliche Fehlhandlungen Schäden verursachen, im schlimmsten Fall wirklich bösartiges Handeln. Die Bandbreite reicht von ungerichteten Angriffen von außen, bei denen Hacker versuchen, in Netze einzudringen, bis hin zu eigenen Mitarbeitenden, die sich bereichern oder dem Unternehmen schaden wollen – etwa aus Rache. In diesen Fällen sind die Schäden meist schlimmer und schwerer zu beherrschen als beim Angriff von außen, denn ein Innentäter kennt die internen Strukturen.

Wie kann man sich schützen?

Frank Rustemeyer: Man kann ganz viele Schutzmaßnahmen ergreifen, die alle ihre Wirkung entfalten: zunächst im technischen Bereich, dann durch Prozesse, also beispielsweise, dass Aufgaben nur im „Vier-Augen-Prinzip“ erledigt werden, ferner durch Vorgaben, durch Kontrollen, durch Schulungen … Nicht für jedes Unternehmen ist es angemessen und wirtschaftlich leistbar, hier auf die allerhöchste Stufe zu zielen. Es ist letzten Endes ein Abwägen zwischen Aufwand und Risiko: Welche Prozesse sind überhaupt IT-abhängig und in welcher Ausfall-Zeit führt das zu welcher Problemklasse? Welche präventiven Maßnahmen kann man ergreifen, die mit überschaubarem Einsatz eine große Schutzwirkung erzielen? Und welches sind Risiken, die man auch sehend in Kauf nehmen kann?

Zur Person

Frank Rustemeyer
Chief Operations Officer (COO)
Geschäftsbereich Security Consulting
HiSolutions AG
Bouchéstraße 12, 12435 Berlin

Das Gespräch führte Antje Borchers, Unternehmenskommunikation der GRB Gesellschaft für Risiko-Beratung mbH.
Ecclesia med GmbH
BDC-Versicherungsservice
Ecclesiastraße 1 – 4, 32758 Detmold
bdc-versicherungsservice@ecclesia.de

Frank Rustemeyer: Als Chief Operations Officer (COO) ist er bei HiSolutions verantwortlich für die Ausgestaltung der operativen Prozesse im Beratungsgeschäft. Außerdem betreut er die Partnerschaft mit der Ecclesia Gruppe und das gemeinsame CyRis-Programm.
HiSolutions ist ein Beratungs- und Dienstleistungsunternehmen, das sich auf die „Sicherheit von Computersystemen“ spezialisiert hat. Es unterstützt Kunden nahezu aller Branchen sowie der öffentlichen Verwaltung dabei, Systeme sicherer zu machen. Bei Schadenfällen oder Cyberangriffen begleitet es Organisationen bei den drei Kernaufgaben: aufklären, was vor sich geht; Schaden begrenzen; wieder in

den normalen Betrieb kommen. Bei HiSolutions arbeiten knapp 200 Mitarbeitende an fünf Standorten, die meisten am Hauptsitz Berlin.

Gemeinsam mit der Ecclesia Gruppe haben Sie das CyRis-Programm entwickelt, das genau so etwas macht: Risiken im IT-Bereich systematisch analysieren, priorisieren, Maßnahmen zur Cybersicherheit festlegen. Was genau bietet das CyRis-Programm für Unternehmen des Gesundheitswesens und der Sozialwirtschaft?

Frank Rustemeyer: Das Thema Cybersicherheit ist komplex. Die Fragen „Wo stehen wir bei unserer Cybersicherheit und was kann schiefgehen?“, sind bei einer Geschäftsleitung oft wenig im Fokus, nicht mal bei den IT-Leuten. Denn die kümmern sich ja vor allem darum, dass der Betrieb läuft. Deswegen haben wir als Einstieg in das CyRis-Programm den CyRis-Basis-Check zur allerersten Standortbestimmung aufgenommen. Das ist ein kleines Projekt, wo ein Fachmann von uns mit viel Erfahrung einen Tag in der Institution verbringt, Gespräche mit verschiedenen Ansprechpartnern führt, sich anguckt: Wie sind die Schutzmaßnahmen aufgestellt? Er vergleicht die Ergebnisse mit seiner Erfahrung und gibt am Ende eine erste Einordnung: „Hier seid ihr gut und da müsst ihr noch was tun.“

Können Schutzmaßnahmen vorbeugend mit den kriminellen Tätern mithalten oder immer nur im Nachhinein Schäden beseitigen?

Frank Rustemeyer: Man kann durchaus mithalten. Allerdings das Ziel „Ich bin immun gegen Angriffe“, das werden wir nicht erreichen. Dazu ist das Themenfeld zu komplex und die Entwicklung viel zu schnell. Aber es ist auch kein Hinterherhechten. Es gibt gute Empfehlungen für Standardschutzmaßnahmen oder wie man ein Sicherheitsmanagement aufsetzt. Natürlich werden sich neue Angriffe entwickeln, auf die man dann nur reagieren kann. Doch so etwas entsteht ja nicht plötzlich, sondern das sind Entwicklungen über Zeiträume, die man beobachten kann.

Empfehlungen für Standardschutzmaßnahmen

Praxistaugliche Checkliste zur Cybersicherheit: www.ecclesia-gruppe.de/Checkliste_Cyber. Darin gibt die Ecclesia zusammen mit HiSolutions einen Überblick über die wichtigsten Handlungsfelder, die auch kleine und mittlere Unternehmen bearbeiten können. Außerdem verweist sie per Links auf die entsprechenden Handlungsempfehlungen zum Beispiel vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

Wie kann ein Unternehmen, das keine IT-Fachleute hat, sein IT-System sicher aufstellen?

Frank Rustemeyer: Die Technik ist nur eines der Elemente eines Schutzkonzeptes. Es gehören auch Prozesse dazu, die die sicherheitskritischen Aufgaben im Unternehmen regeln. Man muss sich als Geschäftsführung darum kümmern, dass diese Prozesse funktionieren: Es muss Leute geben, die sich verantwortlich fühlen; andere Leute, die schauen, wie sich die Technologie weiterentwickelt, auch die Technik im eigenen Hause. Diese Leute planen auch: Was sind die Sicherheitsmaßnahmen, die ich brauche? Und man muss überprüfen, ob die Umsetzung funktioniert. Für die ausführenden Tätigkeiten kann man dann Spezialisten heranziehen – aus dem eigenen Haus oder Dienstleister wie

uns. Natürlich, dafür sind wir da. Aber die Geschäftsleitung muss sicherstellen, dass etwas erfolgt, und muss eben auch am Ball bleiben. Sicherheit ist kein Projekt, das man mal vier Wochen macht und dann als erledigt abheftet.

Wie gut nehmen denn Unternehmen diese Daueraufgabe Sicherheit wahr?

Frank Rustemeyer: Die muss verankert werden in den Organisationen, aber das finden wir sehr wenig. Darum haben wir ein Modul für die Institutionalisierung von Sicherheit geschaffen, die CyRis-Leitlinie. Auch da arbeiten wir in einem Workshop mit dem Unternehmen: Wie könnte ein systematisches Herangehen Ihrer Organisation richtig aufgesetzt werden? Das verschriftlichen wir in einem Papier, der sogenannten Leitlinie.

Stichwort „Sicherheitskultur im Unternehmen". Welchen Anteil hat die am Erfolg eines Schutzkonzeptes?

Frank Rustemeyer: In der Schadenfallsituation macht es einen entscheidenden Unterschied, wie die eigenen Mitarbeitenden reagieren. Darum gehört Training aller Mitarbeitenden dazu, damit sie Risiken erkennen und damit umgehen können. Wenn neue Angriffsvarianten auftauchen, dann kann ein technisches System die nicht erkennen, weil es darauf nicht trainiert ist. Ein Mensch kann, wenn er ein Bewusstsein für die Problematik hat, misstrauisch werden und reagieren.

E-Mail ist immer noch eins der Haupteinfallstore, durch die Schadsoftware in ein Unternehmen gelangt. Woran erkenne ich eine falsche E-Mail? Gibt es fünf Kriterien, die ich anwenden kann?

Frank Rustemeyer: Das gab's früher (lacht): unpersönliche Ansprache, keine Umlaute, schlechtes Deutsch. Das ist viel professioneller geworden. Die E-Mails heute sind meistens in korrekter Sprache und sehr gezielt entworfen, um Schadsoftware zu verbreiten: mit der richtigen Anrede, auch mit einem richtigen Absender, der mit dem Adressaten sowieso in Korrespondenz steht – oft führen die Täter dafür erbeutete Datenbestände zusammen. Wirklich erkennen kann man eine falsche E-Mail meistens nur aus dem Kontext. Wenn man eine E-Mail bekommt mit irgendeinem Anhang, die man nicht erwartet, dann sollte man misstrauisch werden.

Und als Mitarbeiterin soll ich mir nie zu blöd vorkommen, bei der Chefin oder dem Chef oder der IT-Abteilung anzurufen und zu sagen: Hier kommt mir etwas spanisch vor.

Frank Rustemeyer: Genau, Aufmerksamkeit und im Zweifel Nachfragen sind entscheidend. Wenn eine Sicherheitskultur vorherrscht, wo ein Vorfall als persönliches Versagen der Beteiligten geahndet wird, führt das tatsächlich dazu, dass Leute nicht fragen und im Zweifel auch Dinge vertuschen: „Da könnte ich was falsch gemacht haben, da sage ich lieber keinem Bescheid." Das ist fatal für die Sicherheit. Deswegen ermuntern wir, eine Kultur zu etablieren, wo lieber eine Rückfrage zu viel als eine zu wenig gern gesehen wird.

Sie haben Einblick in verschiedenste Unternehmen in unterschiedlichsten Branchen. Erleben Sie da immer wieder dieselben Lücken?

Frank Rustemeyer: Ein Problem, das wir oft sehen, ist die Behandlung von Vorfällen. Selbst wenn man sich mit dem Thema beschäftigt, denkt man vor allem in der Prävention. Es ist aber ganz wichtig, auch zu gucken, was trotz aller Prävention passiert, und daraus zu lernen, Stichwort Incident-Management. Oft treten nur kleine Sicherheitsvorfälle ein, die nicht gleich zu einem Schaden führen. Die soll man nicht irgendwie „wegarbeiten", zum Beispiel einfach den

PC neu aufsetzen, weil das Tagesgeschäft drängt, sondern wirklich prüfen: Was sind die Ursachen für dieses Vorkommnis? Und sei es nur ein merkwürdiger Eintrag in einem Logfile oder eine harmlose Virusinfektion auf irgendeinem PC. Welche Lücken habe ich in meiner Sicherheitskonzeption, die ich schließen muss?

Als Unternehmen sollte ich mich auf einiges vorbereiten, Szenarien durchspielen, damit ich im Schadenfall weiß: Aha, das ist passiert, jetzt muss ich aus der Schublade diesen Plan rausholen und diese Schritte gehen?

Frank Rustemeyer: Unbedingt! Das ist eine Konsequenz aus der Erkenntnis, dass Prävention allein nicht reicht, um das Thema zu erschlagen. Man bewältigt einen eingetretenen Vorfall besser, wenn man vorbereitet ist. Auch dieses Thema ist eines unserer CyRis-Module: Krisenvorsorge, Krisenplanung. Die Fragen dabei lauten: Wer im Unternehmen ist eigentlich dafür zuständig, einen Vorfall zu behandeln? Habe ich so etwas wie einen Krisenstab, wer muss darin vertreten sein? Wo finde ich im Notfall schnell Ansprechpartner für Themen wie rechtliche Beratung, für IT-Forensik, also die technische Unterstützung, für Krisenkommunikation? Wenn ich das alles in Ruhe einmal vorbereite und in einem Plan zusammenschreibe, den ich aus der Schublade ziehen kann, dann spart das enorm Zeit und Stress im Notfall.

Kann man sagen: Unternehmen, die vorbereitet waren und die ihre Aufmerksamkeit erhöht haben, bewältigen Schäden schneller und glimpflicher als andere Unternehmen?

Frank Rustemeyer: Ja, das sehen wir sehr deutlich. Das eine ist die Prävention. Sie soll ja das Eintreten des Schadens unwahrscheinlicher machen. Aber Prävention heißt auch, die Folgen eines eingetretenen Schadens abzumildern. Das klassische Beispiel ist Datensicherung. Die sollte heute selbstverständlich sein, aber auch da erleben wir immer noch interessante Dinge. Wenn also Datenverluste auftreten, dann ist es gut, wenn man eine möglichst frische Sicherung der Datenbestände irgendwo auf einem System hat, das nicht am firmeneigenen Netz hängt, da es sonst vom Angreifer möglicherweise gleich mit manipuliert wird. Es ist auch gut, wenn man mal getestet hat, ob die Datensicherung tatsächlich funktioniert und man Daten zurückspielen kann ins System.

Das andere ist die Art der Krisenreaktion. Geraten Unternehmen in den Panikmodus? Das heißt bei einem Cyberangriff oft: erst einmal alles abschalten! Das allerdings bedeutet Stillstand im Unternehmen. Oder gibt es Prozesse, in denen man zielgerichtet analysiert: Was ist überhaupt gefährdet, wie weit ist der Angreifer gekommen, wen kann ich um Hilfe bitten, wen kann ich einbeziehen in kurzer Zeit? Auch wir von HiSolutions stehen im Rahmen des CyRis-Programms als Krisenhelfer zur Verfügung.

Als Service wäre an dieser Stelle ein kleiner Infokasten mit fünf Tipps gut.

Frank Rustemeyer: Solche Tipps gebe ich ganz bewusst nicht. Denn Cybersicherheit ist zum einen komplex, ist eine Herausforderung, die sich nicht auf fünf Maßnahmen reduzieren lässt. Das andere ist die Gefahr, dass man glaubt, wenn man die fünf Tipps erledigt hat, kann man sich anderen Dingen zuwenden. Das ist genau der falsche Ansatz. Man muss sich mit dem Thema auseinandersetzen. Es gibt Standards in dem Bereich, zum Beispiel vom Bundesamt für Sicherheit in der Informationstechnik. Das sind aber nicht fünf Tipps, sondern umfassende Hilfen.

Aber natürlich gibt es wichtige Maßnahmen:

- das Patchen von Systemen, also das Aktuell-Halten der eigenen Software

- das Einsetzen von Basis-Schutzsystemen wie Antivirus-Firewall
- das Trennen des eigenen Netzes
- das Verschlüsseln von Datenverbindungen und von kritischen/sensiblen E-Mails
- das Sensibilisieren von Mitarbeitenden
- das Behandeln von Vorfällen, also das Incident-Management
- das ständige Anpassen der eigenen Verteidigungsstrategie.

Aber ich glaube, man kann nicht sagen: Mach das so! Es kann für jede Organisation andere Wege geben.

Rustemeyer F: „Sicherheit ist kein Projekt, das man mal vier Wochen macht.“ Passion Chirurgie. 2020 Januar, 10(01): Artikel 04_04.

Autor des Artikels

Ecclesia Versicherungsdienst

BDC-Versicherungsservice
Telefon 0800/603-6030
Ecclesiastraße 1-4
32758 Detmold
> kontaktieren