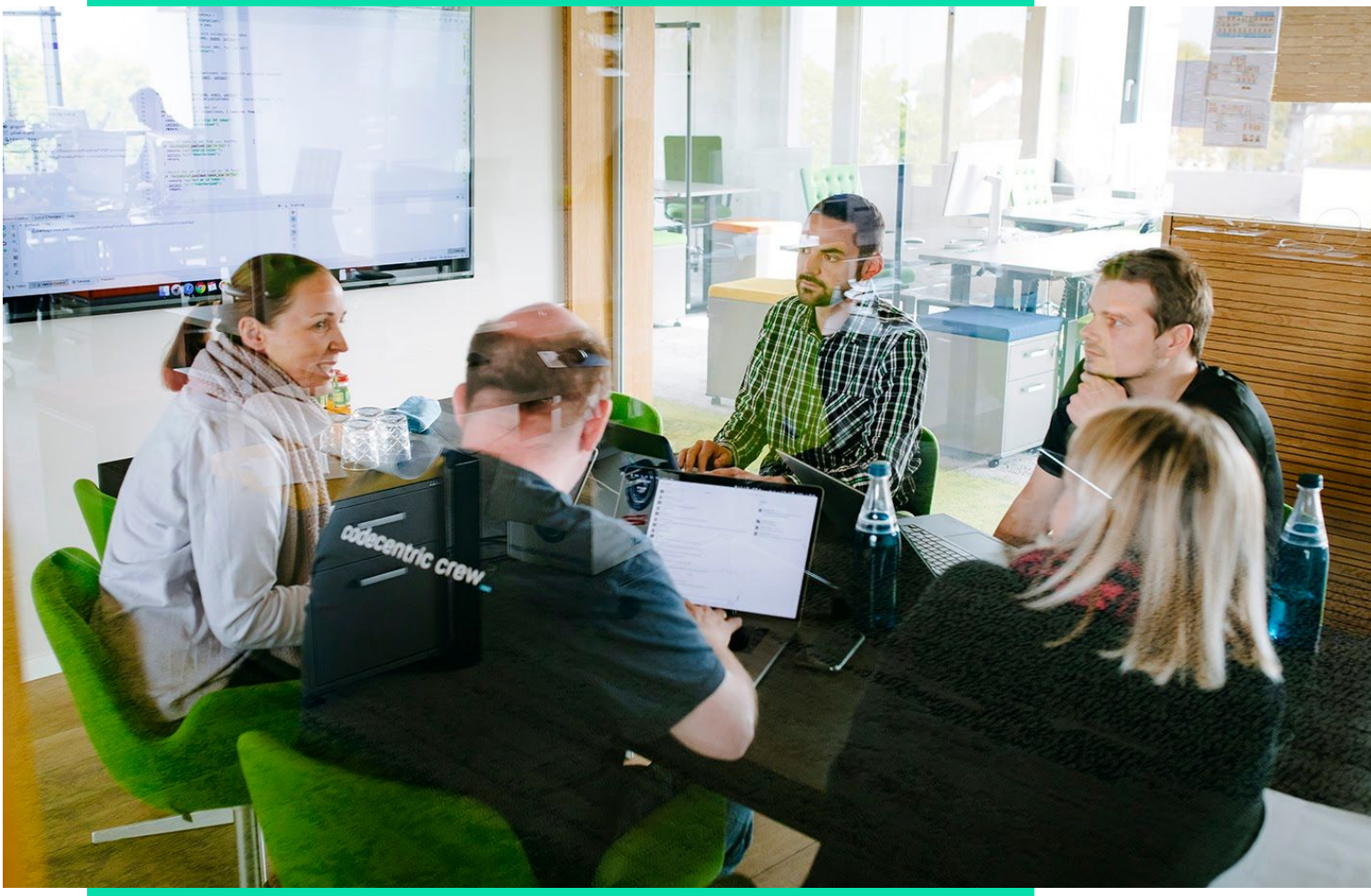
codecentric stories



Digitalisierungsprojekte richtig aufstellen: Security

Die fünf Säulen der Sicherheit, oder: Wie integriert man IT Security in ein Unternehmen?

Die Vorteile aber auch die Notwendigkeit digitaler Transformation liegen auf der Hand: Digitalisierung bietet neue Geschäftsmodelle, erlaubt neue Formen der Kollaboration und verbesserte Customer Experience, um nur einige zu nennen. Aber Digitalisierung bedeutet zunächst vor allem Herausforderungen. Im Zuge unserer Kolumne haben wir bereits den Veränderungsprozess genauer betrachtet, den Unternehmen durchlaufen müssen. In diesem Artikel wollen wir einmal mehr auf die technischen Herausforderungen schauen. Genauer gesagt, auf einen häufig immer noch vernachlässigten Aspekt von IT-Systemen: die Security. Als wäre es für Fachabteilungen nicht bereits hochkomplex ihre bestehenden IT-Systeme zeitgemäß zu machen, lauern Hacker nur darauf, dass Fehler gemacht und so Tür und Hof für Angriffe geöffnet werden.

Die schlechte Nachricht zuerst

Die IT-Infrastruktur jedes Unternehmens kann und wird das Ziel von Hackern werden. Die Frage lautet nicht, *ob* es passiert, sondern *wann* und *wie*.
Manche sagen, es gibt eigentlich nur zwei Arten von Unternehmen: Solche, die schon einmal gehackt worden sind – und solche, die nicht wissen, dass sie schon gehackt worden sind. Die Bedrohung ist real.
Und da eigentlich jedes Unternehmen von einer funktionierenden und vernetzten IT-Infrastruktur abhängig ist, sollte man annehmen, dass alle die notwendigen Maßnahmen für mehr Sicherheit ergreifen, richtig? Leider ist das offenbar nicht Fall, wie wir in unserer täglichen Arbeit immer wieder feststellen müssen.

Warum bereiten sich die Firmen nicht vor?

Die meisten Manager*innen würden zustimmen, dass IT Security hochgradig wichtig ist. Aber in der Realität haben viele Firmen dann doch nicht die Mittel, um einem Angriff zu begegnen – oder einen solchen überhaupt erst einmal zu erkennen.

Der wahrscheinlich wichtigste Grund dafür: Geld. IT Security kostet sehr viel Geld. Für ein großes mittelständisches Unternehmen können die jährlichen Kosten durchaus eine Million Euro übersteigen. Ein voll ausgerüstetes „Security Operation Center" (SOC) benötigt mindestens 9 bis 12 Mitarbeiterinnen und Mitarbeiter, die 24/7 zur Verfügung stehen. Und das ist leider erst der Anfang.

Auf der anderen Seite gibt es Kostenblöcke in ähnlicher Größenordnung, die ein Unternehmen sehr wohl bereitwillig zahlt. Warum also wird IT Security häufig vernachlässigt? Warum implementieren IT-Abteilungen nicht die notwendigen Sicherheitsmechanismen, um vorbereitet zu sein?

Aber warum sollten es Angreifer ausgerechnet auf Ihr Unternehmen absehen?

Es gibt einfach zu viele Angreifer da draußen, angefangen mit automatischen Bots, die einfach jede IP-Adresse und jeden Port nach allgemeinen Schwachstellen absuchen. Solche Angriffe richten sich häufig noch nicht einmal direkt an Sie; dass Ihre Firma getroffen wird, kann auch einfach nur ein Kollateralschaden sein.

Das beste – oder eigentlich das schlimmste – Beispiel dafür ist der Hackerangriff auf die Uniklinik Düsseldorf im September 2020 – ein Angriff mit tödlichem Ausgang für mindestens eine betroffene Person. Und eigentlich ging es um ein ganz anderes Ziel.

Neben automatischen Bots gibt es eine ganze Menge an Personen und Gruppierungen mit höchst unterschiedlichen Absichten. Die Bandbreite reicht vom Nervenkitzel oder dem Spaß in ein fremdes Netzwerk einzubrechen, über die Benutzung von Rechenkapazität zum Minen von Bitcoins, direktem finanziellen Gewinn (z. B. durch Datendiebstahl oder Lösegeldforderungen), über Spionage oder der Beschädigung von Mitbewerbern durch „Denial of Service"-Angriffe (DoS) bis hin zu Staaten, die Hacking für politische Ziele einsetzen – alles ist denkbar und möglich.

Es ist größtenteils ein Management-Problem

Viele Manager*innen verstehen die Kritikalität der Bedrohung nicht wirklich; sie haben einfach nicht das technische Verständnis dafür. Also halten sie sich an Plattitüden, ohne diese wirklich zu glauben.
Oder: Sie verstehen sie sehr wohl, wollen aber nicht die Unannehmlichkeiten in Kauf nehmen, die IT Security häufig mit sich bringt, wenn man es nicht richtig macht. Ein komplexes Passwort zum Beispiel, zusammen mit Multi-Faktor-Authentifizierung (MFA) ist deutlich aufwändiger, als einfach „1234" oder „admin123" einzugeben, wenn man sich anmelden möchte.

Dieses Verhalten ist gefährlich

Ein erfolgreicher Hacker-Angriff auf eine Firma kann sehr teuer werden. Die Kosten, wenn in großem Stil Daten gestohlen werden, können sich leicht in 6-, 7- oder sogar 8-stelliger Größenordnung bewegen; nicht eingerechnet, die möglichen Strafzahlungen wegen Verstoß gegen die DSGVO (Datenschutzgrundverordnung) oder anderer Regularien.

Ein Angriff kann auch die IT-Infrastruktur so sehr schädigen, dass im Extremfall die gesamte Firma den Betrieb einstellen muss. Fragen Sie sich selbst: Wie lange können Ihre Geschäftsprozesse ausschließlich auf Basis von Papier ohne Computer überstehen?

Aber IT Security kann nicht einfach zu einer bestehenden Infrastruktur hinzugefügt werden. Sie ist nicht einfach ein Produkt, das man kaufen und installieren kann. „Bitte baut mir erst alle Features, wir können Sicherheit später dazu packen", funktioniert einfach nicht. Ganz und gar nicht.

Die fünf Säulen der Sicherheit

Tatsächlich muss IT Security in eine Organisation integriert sein, um Wirkung zeigen zu können. Sie ist nicht einfach nur ein „Additiv".
Gute IT Security besteht mindestens aus diesen fünf Elementen:

Sichtbarkeit

Ein Unternehmen muss einen sich anbahnenden oder stattfindenden Angriff bemerken und verfolgen können. Das bedeutet, dass die gesamte technische Infrastruktur mit Sensoren ausgestattet sein muss. Meisten laufen dann Softwareagenten – kleine Sensorprogramme – auf jedem Laptop, Desktop Computer, Server, auf der Firewall, auf jedem Router oder Switch und auf allen anderen Komponenten, aus denen Ihr Netzwerk besteht. Alle Systeme müssen in der Lage sein, unnormales Verhalten zu bemerken und alles zu reporten, was auf der Maschine vor sich geht. Spannenderweise bringt Windows 10 „Out of the box" schon sehr viel davon mit. Aber die meisten dieser Features sind per Werkseinstellung abgeschaltet – vermutlich, um kompatibel mit älteren Versionen zu sein.

Alle Logfiles, Ereignisprotokolle und Berichte der Agenten müssen dann in einem System namens SIEM (Security Information and Event Management) zusammengefasst und konsolidiert werden. Ein SIEM kann die Vorgänge auf den unterschiedlichen

Systemen korrelieren und dadurch weitere Abweichungen von der Norm feststellen, die unentdeckt bleiben würden, wenn man sich nur einen Computer alleine anschaut.
Wie Sie sich vorstellen können, benötigt ein SIEM sehr viel Speicherplatz. Die Logfiles von jedem Computer zu sammeln und für Tage oder Wochen zu speichern ergibt viele Terabytes an Daten. Aber es lohnt sich.
Natürlich braucht es auch Menschen, die diese Systeme rund um die Uhr überwachen. In einem Security Operation Center (SOC) wird das SOC Level I genannt und besteht mindestens aus drei Schichten von ausgebildeten Mitarbeiterinnen und Mitarbeitern, die die Alarmsysteme überprüfen und erste Analysen vornehmen können.

Untersuchen / Analysieren

Bemerken die Sensoren etwas, muss das SOC die Situation bewerten. Die Systeme finden in der Regel deutlich mehr Fehlalarme als echte. Diese „False Positives“ müssen aussortiert und geschlossen werden.
Wenn das SOC dann einen echten Angriff feststellt, wechselt es in den „Incident Response“-Modus. Das bedeutet, das Verhalten der Angreifer zu analysieren und zu verstehen, um dann die notwendig Maßnahmen dagegen ergreifen zu können.
Das nennt man SOC Level II. Dazu ist sehr viel Wissen über Betriebssysteme und deren Konfiguration, das Verhalten von Hackern, bestehende Schwachstellen in Systeme oder übliche Vorgehensmodelle von Angreifern erforderlich, kombiniert mit tiefem Verständnis der IT-Systeme des Unternehmens. Ein SOC muss genau wissen, welche Systeme wie kritisch sind: Was kann einfach abgeschaltet werden, und was muss geschützt werden, koste es was es wolle? Dafür benötigt das SOC eine BIA (Business Impact Analysis).

Durchführen / Agieren

Man könnte meinen, SOC I und SOC II sind ausreichende Einheiten für einen Sicherheitsvorfall. Aber jedes SOC kann nur so effektiv sein, wie dessen Pläne und Empfehlungen auch tatsächlich von der IT umgesetzt werden. Wenn ein SOC anweist, das Unternehmen vom Internet zu trennen, dann muss da jemand sein, der alle Zugangspunkte kennt und sie abschalten kann. Wenn das SOC Informationen zur Nutzung einzelner Server benötigt oder das Image eines Rechners, um dieses forensisch zu analysieren, dann muss die Serviceorganisation der IT liefern können.

Ohne ein schlagkräftiges Service Desk kann ein SOC nichts ausrichten. Ein Unternehmen braucht also auch ein funktionierendes Ticket-System, Priorisierungsregeln und verfügbares, ausgebildetes Personal.

Governance

Dieses Wort klingt sehr sperrig, also formulieren wir es um: IT Security muss einen prominenten Platz in der Organisation haben – und nicht nur in der IT-Abteilung. Ihr Unternehmen muss einen Chief Information Security Officer (CISO) bestellen, der viel Erfahrung hat und mit ausreichender Entscheidungsbefugnis ausgestattet ist. Ein CISO kann nicht immer erst den Vorstand befragen; im Falle eines Sicherheitsvorfalls bleibt dazu häufig nicht die Zeit.
Daneben braucht es noch Sicherheitsregeln, die das Unternehmen beschützen, z. B.: Welche Systeme sollen wie konfiguriert werden? Welche Kommunikationsprotokolle ins Internet werden benötigt, und welche werden blockiert?
Besonders wichtig ist es, eine IT-Sicherheitsabteilung nicht als „Department of NO“ zu installieren. Das bedeutet, dieser Bereich soll nicht einfach nur als eine Art interner TÜV unsichere Lösungen ablehnen, sondern durch entsprechende Beratung Anderen helfen, sichere Lösungen zu erstellen. Das betrifft jeden in der IT, das Management, die Entwicklung, den IT-Betrieb oder den Netzwerk-Bereich. IT-Security-Abteilungen und Berater sind „Enabler”, sie helfen den Kolleg*innen und Projekten besser zu werden.
Schließlich ist das Bewusstsein der gesamten Belegschaft für IT Security entscheidend. Jeder einzelne Mitarbeiter und jede einzelne Mitarbeiterin muss das Risiko von Phishing kennen und wissen, wie man solche E-Mails erkennt. Der Mensch ist das schwächste Glied in der Kette und wird es wohl auch bleiben. Ein Unternehmen muss auch in die Ausbildung aller Mitarbeiter*innen investieren.

Threat hunting

Wenn alle vorher genannten Elemente platziert sind – Sie können ungewöhnliches Verhalten der Computer erkennen, Sie können diese aktiv analysieren und Gegenmaßnahmen einleiten, und Sie haben auch Regeln und Richtlinien, an denen man sich orientieren kann –, dann beginnt die Jagdsaison!
Es wird Zeit, ein IT Security Threat Hunting Team zu etablieren. So ein Team wird auch SOC Level III genannt. Ein SOC III sucht aktiv und ohne bestehenden Hinweis nach Schwachstellen und unerkannten Problemen. Das Ziel ist es, permanent die Erkennung und Beseitigung von Bedrohungen zu verbessern, zum Beispiel indem die etablierten Standardlösungen und -verfahren ausprobiert und verprobt werden.

Ein SOC III führt zum Beispiel Penetrationstests von außen auf die IT-Infrastruktur durch, scannt das interne Netzwerk nach falsch konfigurierten Maschinen oder untersucht Ketten von Zugriffsrechten, die von Angreifern gerne ausgenutzt werden (sogenanntes „Lateral Movement“). Ein Threat Hunting Team nimmt die Rolle eines Angreifers ein, um Schwachstellen zu finden bevor ein Hacker es tut.

IT-Sicherheit ist ein organisatorisches Thema

Jedes Unternehmen muss die oben genannten fünf Elemente auf die eine oder andere Weise etablieren. Keine Organisation kann es sich noch leisten, IT Security nicht als geschäftskritisch anzusehen. Das gesamte Unternehmen hängt davon ab. IT Security wird zu Veränderungen im System führen, es muss tief in die gesamte Organisation eingebettet sein.
Ja, das kostet eine Menge Geld. Doch ein aufmerksames und schlagkräftiges SOC-Team und eine IT-Organisation, die schnell reagieren kann, können gemeinsam den Unterschied ausmachen. Sie können einen Angriff frühzeitig verhindern oder beenden, bevor ein Hacker frei durch das Netzwerk spaziert, Daten kopiert, um sie im Darknet zu verkaufen und anschließend alle Computer verschlüsselt, um Lösegeld zu erpressen.
Je schneller Ihr Unternehmen eine wirksame IT Security aufbaut, desto besser können Sie Angreifer voraus sein. Und das kann letztendlich sehr viel Geld sparen.
Auch im Falle eines IT-Sicherheitsvorfalls gilt das, was im „klassischen“ Business gilt:

ZEIT IST GELD!

codecentric stories ist eine Kolumne der codecentric AG, in der wir von unseren Erfahrungen berichten, Denkanstöße geben und Lösungsansätze diskutieren möchten. Unsere Beobachtungen haben keinen Anspruch auf Vollständigkeit oder Wissenschaftlichkeit.

Autor

Goetz Markgraf
Product Owner

goetz.markgraf@codecentric.de