49187

IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Datenschutz

2|2017

Thomas Schneider,
IT-Security Engineer bei mod IT Services

„Wann ist eine Infrastruktur kritisch?“

Cloud Security Normen, Verschlüsselungstipps, Microservices & more
IAM Kunden und soziale Netze erfolgreich einbeziehen
Technik Blockchain-Technologie revolutioniert das digitale Business

DATAKONTEXT

www.itsicherheit-online.com

EIN RECHTSRAHMEN ZUR BESTIMMUNG FÜR KRITISCHE INFRASTRUKTUREN

WANN IST EINE INFRASTRUKTUR KRITISCH?

Seit gut zwei Jahren gilt in Deutschland das IT-Sicherheitsgesetz. Es beinhaltet Richtlinien und Vorgaben, wie zum Beispiel, dass Unternehmen IT-Angriffe sowie Datenschutzpannen den Behörden melden müssen oder die eingesetzte Soft- und Hardware störungsfrei und sicher nach dem Stand der Technik betrieben werden soll. Doch wer muss sich an dieses Gesetz halten? Und was bedeutet es konkret für Unternehmen und Branchen?

Im Mai 2016 veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Verordnung zur Bestimmung Kritischer Infrastrukturen (Kritis-Verordnung). Ziel war es, das bis dahin in diesem Punkt zu vage gebliebene IT-Sicherheitsgesetz zu konkretisieren. Diese Kritis-Verordnung beschreibt und definiert welche Branchen – und daraus resultierend welche Unternehmen – unter das IT-Sicherheitsgesetz fallen. Der erste Teil der Verordnung befasst sich mit Betreibern und demnach Unternehmen sogenannter kritischer Infrastrukturen, wie Energie- und Wasserversorger, Telekommunikations-Dienstleister und Nahrungsmittelproduzenten. Der zweite Teil der Kritis-Verordnung widmet sich dem Finanz- und Versicherungswesen, Transport und Verkehr und Unternehmen aus dem Bereich der medizinischen Versorgung.

Was ist eine kritische Infrastruktur und in welchem Fall ist diese wirklich kritisch?

Die Kritis-Verordnung selbst beinhaltet in erster Linie keine IT-Vorgaben oder definiert Anforderungen an IT-Sicherheitsstandards. Vielmehr dient sie als Mittel zur Bestimmung und Definition ob Unternehmen grundlegend als Betreiber kritischer Infrastrukturen gelten. Dabei geht es nicht um IT-Infrastrukturen als solche oder um deren kritische Komponenten, wie zum Beispiel Firewall- oder Anti-Virus-Systeme. Es sind kritische Infrastrukturen im Sinne des staatlichen Gemeinwesens beziehungsweise der Versorgung der Allgemeinheit durch Leistungen definierter Sektoren gemeint, „deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde" (vgl. BSI-KritisV, § 1).

Die Methodik zur Bestimmung dieser Infrastrukturen erfolgt anhand der Verordnung mehrstufig Sie definiert zunächst Begrifflichkeiten wie Versorgungsgrad oder Betreiber, beschreibt weiter sektorspezifische sowie die als kritisch einzuordnenden Dienstleistungen und nennt abschließend Schwellenwerte eines jeweiligen Sektors, ab denen Leistungen als kritisch gelten. Die Anhänge der Kritis-Verordnung beinhalten tabellarische Angaben für Anlagekategorien und Schwellenwerte sowie Berechnungsformeln zur Ermittlung der Schwellenwerte.

Für die Sektoren Energie und Wasser werden dabei Angaben sowohl bezüglich der Versorgungs- als auch der Fördermengen gemacht. Der Sektor Informationstechnik und Telekommunikation beinhaltet Angaben zur Daten- und Sprachübermittlung sowie zur Datenverarbeitung und -speicherung. Der Sektor Ernährung enthält Schwellenwerte zu den Bereichen der Lebensmittelversorgung, -produktion, -distribution und -bereitstellung. Die Sektoren Verkehr und Transport, Finanz- und Versicherungswesen sowie Gesundheit erhalten ihre sektorspezifischen Definitionen erst mit dem zweiten Teil der Kritis-Verordnung. Nach Angaben des BSI soll dieser noch im Frühjahr 2017 erscheinen.

Treffen Definition und Schwellenwerte nach Kritis-Verordnung für Unternehmen zu, so sind diese als Betreiber kritischer Infrastruk-

turen anzusehen. Unternehmen werden also dazu verpflichtet sowohl organisatorische als auch technische Maßnahmen als Mindest-Sicherheitsstandards konform mit dem IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) nach dem Stand der Technik zu etablieren. Dafür haben die Gesetzgeber einen festen Zeitrahmen vorgegeben: Zwei Jahre nach Inkrafttreten der Verordnung – sprich im Mai 2018 – wird die Einhaltung der Anforderungen zur Pflicht Ab diesem Zeitpunkt drohen dann Bußgelder, wenn dem nicht nachgekommen wird.

Konkrete praktische Auswirkungen

Das klingt zunächst vage, denn was bedeutet „Stand der Technik" genau und welche Maßnahmen sind konkret gemeint? Der Begriff „Stand der Technik" ist tatsächlich ein bewährter juristischer Begriff, da die technische Entwicklung deutlich schneller voranschreitet als die Gesetzgebung. Der Begriff selbst verweist auf bereits bestehende internationale und nationale Normen wie DIN- oder ISO-Standards, die aktuelle technische und organisatorische Maßnahmen, Komponenten sowie Prozesse definieren Diese können sich jedoch je nach Branche, Unternehmen oder Einzelfall unterscheiden. Die in der Kritis-Verordnung definierten Unternehmen und entsprechende Branchenverbände sind deshalb dazu angehalten, branchenspezifische Standards eigenständig zu definieren und durch das Bundesamt prüfen zu lassen.

Aus diesen Standards lassen sich die Maßnahmen direkt ableiten. Beispielsweise bietet das BSI hier eine Zertifizierung nach ISO 270001 auf Basis des IT-Grundschutzes an. Dieses beschreibt, wie Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) ganzheitlich in einem Unternehmen durch die Umsetzung sowohl organisatorischer (Richtlinien, Verfahren, Prozesse sowie Rollen) als auch technischer Maßnahmen gewährleistet werden kann.

Die ISO-Standards und auch das IT-Grundschutz-Regelwerk fassen alle diese Maßnahmen unter dem Begriff Informationssicherheitsmanagement-System (ISMS) zusammen. Darüber hinaus definiert ein ISMS Prozesse zur Risikominimierung innerhalb der IT-Umgebung auf technischer Basis. Damit ist unter anderem eine Lösung gemeint, die systematisch Schwachstellen aufdeckt. Denn allein Prozesse und spezialisierte Rollen zur Vermeidung von Cyber-Angriffen reichen nicht aus, wenn kein transparenter Blick auf den technischen IST-Zustand und somit potenzielle oder gar bereits vorhandene Risiken besteht.

Ein etabliertes und umfassendes Schwachstellen-Management ist gerade in zunehmend komplexen IT-Strukturen eine effektive Methode, um nicht nur einzelne Komponenten wie etwa Firewalls oder Ähnliches, sondern vielmehr das gesamte Netzwerk regelmäßig und fortlaufend gezielt auf bekannte Lücken, Konfigurationsfehle , fehlende Updates oder veraltete Betriebssysteme hin zu überprüfen. Die Ergebnisse solcher Scans können wiederum die Basis für eine weitere Absicherung der Infrastruktur sein. Ein Schwachstellen-Management kann so innerhalb eines ISMS als grundlegender Bestandteil einer sicheren IT-Umgebung fungieren.

Für „Nicht-Kritis-Unternehmen" ebenso wichtig

Unternehmen, die die Schwellenwerte der Kritis-Verordnung nicht erreichen, sind dem Gesetz gegenüber nicht verpflichtet – auch wenn sie in denselben Sektoren Dienstleistungen und Services anbieten oder als Zulieferer fungieren. Der Gedanke, man müsse sich deshalb keine Sorgen machen, bietet sich an. Zwar können diese Unternehmen faktisch auch weiterbestehen, ohne die Kritis-Anforderungen einzuhalten. Jedoch ergeben sich gewisse Abhängigkeiten und Wechselwirkungen, da Kritis-konforme Unternehmen durch Etablierung neuer Sicherheits-Standards angepasste oder gar komplett neue Anforderungen an ihre Zulieferer, Entwicklungs- sowie Kooperationspartner haben. Soll heißen: Auch die Geschäftspartner von Kritis-Unternehmen werden vielfach die Kritis-Anforderungen einhalten müssen, um Partner bleiben zu können.

Tatsächlich stellt das IT-Sicherheitsgesetz aber auch eine gute Sicherheits-Definition für Unternehmen dar, die die Schwellenwerte der Kritis-Verordnung nicht erreichen und deshalb nicht als kritisch gelten – jedenfalls nicht vor dem Gesetz. Doch auch die Leistungen kleinerer Unternehmen werden schnell gesellschaftskritisch, wenn nur die richtigen Sektoren betroffen sind. Ein Beispiel: Jedes Krankhaus hat unzählige Zulieferer, kleine und große, generalistische und hoch spezialisierte. Nur einige davon werden künftig per Gesetz zur Einhaltung des IT-Sicherheitsgesetzes verpflichtet werden. Wenn aber aufgrund einer IT-Sicherheitspanne das lebensrettende Medikament nicht pünktlich geliefert werden kann, wird der Lieferant zum Teil des kritischen Systems. Unternehmen, die Kritis-Konformität erreichen möchten, ohne offiziell betroffen zu sein, können dem sogenannten UP Kritis, der öffentlich-privaten Kooperation zwischen Betreibern Kritischer Infrastrukturen, beitreten und unter anderem bei der Gestaltung gewisser Branchenstandards mitwirken.

Die Frage, wann eine Infrastruktur kritisch ist, lässt sich nicht einfach beantworten. Zwar schafft das IT-Sicherheitsgesetz mit Hilfe der Kritis-Verordnung hier einen Rahmen, indem es Schwellenwerte definiert und damit entsprechend die betroffenen Unternehmen indirekt benennt. Aber auch alle anderen Unternehmen sollten sich mit den Anforderungen beschäftigen. Zum einen ergeben sich aus Branchenstandards immer Wettbewerbskriterien. Dabei ist es stets von Vorteil, man gestaltet mit, statt zurückzubleiben. Zum anderen geht es schlicht um eine umfassende IT-Sicherheit: Diese sollte heute ein fester Bestandteil jeder Unternehmenskultur sein und mittels etablierter Prozesse und mit modernen Werkzeugen umgesetzt werden.

THOMAS SCHNEIDER,
IT-Security Engineer bei mod IT Services

„SYSTEMATISCHES SCHWACHSTELLEN-MANAGEMENT **LOHNT SICH**“

Interview mit Sebastian Brabetz, Teamleader Professional Security Solutions bei mod IT Services

Das IT-Sicherheitsgesetz verpflichtet Betreiber kritischer Infrastrukturen, Verfahren umzusetzen, die IT-Sicherheitsrisiken minimieren sollen. Der Gesetzestext geht dabei nicht auf konkrete Maßnahmen ein. IT-Sicherheits-Experte Sebastian Brabetz von mod IT Services empfiehlt Unternehmen, IT-Risiken nicht nur punktuell zu bekämpfen, sondern ein umfassendes Schwachstellen-Management zu etablieren. Warum und wie das funktionieren soll, erläutert er im Interview.

ITS: Das IT-Sicherheitsgesetz ist noch immer nicht richtig ausdefiniert, dennoch wirft es kaum zu ignorierende Schatten voraus. Warum sollten sich Betreiber kritischer Infrastrukturen unbedingt mit dem Thema beschäftigen?
Sebastian Brabetz: Das hat gleich mehrere Gründe: Vor allem ist IT-Sicherheit natürlich per se ein geschäftskritisches Thema. Zwar muss heute kaum noch ein Unternehmer oder Manager davon überzeugt werden, sein Augenmerk hierauf zu legen. Doch in der Praxis stellen wir immer wieder fest, dass zwar Firewalls und ähnliche Standardwerkzeuge gut gemanagt werden, IT-Sicherheit aber noch immer nicht ganzheitlich betrachtet wird. Das heißt, es gibt kaum regelmäßige Sicherheitsaudits oder definierte Prozesse, die dann greifen, wenn es zu einem IT-Sicherheitsvorfall gekommen ist. Für Betreiber kritischer Infrastrukturen ist das doppelt brisant: Eben weil sie kritische Infrastrukturen bereitstellen, sind sie für Hacker natürlich besonders interessant. Zugleich kann ein Ausfall der IT extreme Folgen haben. So kann das E-Werk seine Anwohner nicht mehr mit Strom versorgen oder der Betrieb im Krankenhaus ist eingeschränkt – alles deutlich schlimmer, als wenn ein Dienstleistungsunternehmen für einen halben Tag keinen Zugriff auf seine E-Mails hat. Und dann wäre da ja auch noch der Gesetzgeber als kontrollierende Instanz. Dieser kann und wird die Einhaltung des IT-Sicherheitsgesetzes einfordern. Es bleibt nicht mehr viel Zeit: Ab Mai 2018 ist das Gesetz verpflichtend.

ITS: Die Kritis-Verordnung definiert anhand von Schwellenwerten, welche Unternehmen vom IT-Sicherheitsgesetz betroffen sind. Heißt das, dass sich Unternehmen zurücklehnen können, die diese Schwellenwerte nicht erreichen, auch wenn sie in denselben Bereichen – wie etwa Strom- oder medizinische Versorgung – tätig sind?

Sebastian Brabetz: Das wäre aus meiner Sicht zu kurz gedacht. Zwar werden die Unternehmen im Falle eines Falles von offizieller Seite keine Bußgelder oder Ähnliches zu befürchten haben. Ich möchte jedoch davor warnen, die Vorgaben des IT-Sicherheitsgesetzes nur als etwas zu sehen, was jetzt auch noch erfüllt werden muss. Es geht um viel mehr: Es geht um das Bewusstsein für eine umfassende IT-Sicherheit über die rein technische Absicherung der IT-Infrastruktur hinaus. Es geht um Prozesse und ein echtes Management der IT-Sicherheit. Soll heißen: Selbst wenn Unternehmen möglichweise nicht per Definition unter das IT-Sicherheitsgesetz fallen, sollte IT-Sicherheit als geschäftskritisches Thema die notwendige Aufmerksamkeit bekommen.

ITS: Wie sieht so ein umfassendes Bewusstsein für IT-Sicherheit in der Praxis aus?

Sebastian Brabetz: Die Basis bilden technische Maßnahmen, wie zum Beispiel ein Patch- und Updatemanagement, Firewalls, Penetrationstests oder die Segmentierung der Infrastruktur entsprechend verschiedenen Anforderungen an Datenschutz und Datensicherheit. Aber dass all diese Maßnahmen, auch wenn sie noch so ernsthaft betrieben werden, nie alle Lücken auf Dauer schließen können, ist kein Geheimnis. IT-Sicherheit braucht ein umfassendes Schwachstellen-Management, welches in regelmäßig stattfindende Prozesse gegossen ist und das auch die Fachabteilungen und Management-Ebenen mit einbezieht. So sollte beispielsweise eine Risikoanalyse über alle bestehenden Systeme hinweg durchgeführt werden. Denn nicht nur die kritischen Infrastrukturen selbst benötigen eine entsprechende Absicherung, sondern auch die Rechner, mit denen Mitarbeiter in der Zentrale etwa Daten zur Auswertung ziehen. Zwar mögen solche Projektsteuerungsaufgaben selbst weniger kritisch sein, die IT-Technik kann aber zum Einfallstor werden. Die Definition von vorbeugenden Maßnahmen ist ebenso wichtig wie die von Prozessen, die im Krisenfall greifen. Jeder Mitarbeiter muss dafür sensibilisiert sein, was zu tun ist, wenn zum Beispiel Malware eingeschleust wurde, oder wann Daten sensibel sind und wie damit umzugehen ist.

ITS: Können und sollten die konkreten Maßnahmen in vorhandene IT-Sicherheitskonzepte integriert werden?

Sebastian Brabetz: Bei der Analyse vorab sollte man auf jeden Fall vorhandene Maßnahmen, Prozesse und Zuständigkeiten berücksichtigen. Es gibt kaum mehr ein Unternehmen, bei dem IT-Sicherheit nicht bereits ein Thema ist – auf einer vorhandenen Basis lässt sich gut aufsetzen. Eine umfassende Risikoanalyse klärt darüber hinaus, welche Infrastrukturbereiche welche Schutzlevel benötigen. Welche Bedrohungen sind real und mit welchen Mitteln sowie welchem Aufwand kann man sich dagegen sinnvoll schützen? Es geht dabei auch um die ehrliche Erkenntnis, dass es nicht möglich ist, alle Lücken komplett zu schließen. Mit welchem Risiko muss man also leben und was ist schließlich zu tun, wenn der Fall X eintritt? Malware ist so eine Bedrohung, der wohl nie ganz beizukommen ist. Doch wenn es klare Regelungen gibt, was zu passieren hat, falls die schadhafte E-Mail nun doch geöffnet wurde und der betroffene Mitarbeiter dies auch weiß, dann kann der Schaden stark eingegrenzt werden.

ITS: Wie viel Aufwand ist es, ein professionelles und systematisches Schwachstellen-Management im Unternehmen zu etablieren? Lohnt sich das?

Sebastian Brabetz: Dass die Umsetzung eines sinnvollen Schwachstellen-Managements mit Aufwand verbunden ist, lässt sich nicht bestreiten. Gute Vorbereitung ist hierbei immens wichtig. Am Beispiel einer konkreten Maßnahme – des Schwachstellenscans – möchte ich erläutern, warum das so ist und warum es sich lohnt, sich diese Gedanken zu machen: Auch wenn bereits ein Tool ausgewählt wurde, sind einige weitere Vorbereitungen notwendig. Zum Beispiel die Frage, wer seitens der IT-Abteilung noch mit einzubeziehen ist. Denn Schwachstellenscans werden von Security- und Monitoring-Systemen häufig als Angriff identifiziert und produzieren jede Menge Logs sowie False Positives – die operativen Administratoren und Spezialisten für Intrusion Prevention und Intrusion Detection System (IPS und IDS) sowie ähnliche Systeme sollten informiert sein, um die Ereignisse richtig deuten zu können. Werden Teile der Infrastruktur extern gehostet, müssen Genehmigungen eingeholt und Absprachen mit dem Provider getroffen werden. Manche Produktionssteuerungssysteme können dabei nicht ohne weiteres gescannt werden, da sie als Embedded Systems besonderen Hersteller-Auflagen unterliegen. Auch Produktionszyklen entscheiden unter Umständen über das günstigste Zeitfenster für einen Scan. Schließlich benötigen die individuelle Anpassung des Scanners und die Auswertung der Ergebnisse entsprechend Zeit. Und dann sollte aus dem einmaligen Scan ein regelmäßiger Prozess gemacht werden.

Lange Rede, kurzer Sinn: Der Aufwand ist am Anfang deutlich höher, gut durchdacht und systematisch aufgesetzt nimmt dieser aber schnell ab. Langfristig gedacht senkt ein sinnvoll aufgesetztes Schwachstellen-Management das Risiko deutlich.

ITS: Herr Brabetz, vielen Dank für das Gespräch!

Das Interview führte Stefan Mutschler, stellvertretender Chefredakteur IT-SICHERHEIT