# IT-Sicherheitsgesetz

## Die nächste Phase wird eingeläutet

Kai-Oliver Detken

Durch die zunehmende Zahl der Terroranschläge wird weltweit seit einigen Jahren ein erhöhter Schutz kritischer Infrastrukturen (Kritis) vor Cyberattacken gefordert. Darunter gehören Anlagen, Systeme oder Teile, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen sind. Aus diesem Grund trat am 25. Juli 2015 ein Artikelgesetz zur Erhöhung der Sicherheit informationstechnischer Systeme in Kraft, das für das BSI eine zentrale Rolle vorsieht und den betroffenen Unternehmen neue Anforderungen für das Monitoring und die Meldung von Sicherheitsvorfällen vorschreibt. Während man in der Übergangsphase noch „Augen zugedrückt" hat, sollen in Zukunft Kritis-Betreiber stärker auf die Einhaltung der Gesetzesvorlagen kontrolliert werden. Hierbei stellt sich allerdings die Frage, ob Behörden und Firmen gleichermaßen ausreichend darauf vorbereitet sind.

*Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen*

Mit dem Beschluss des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (kurz: IT-Sicherheitsgesetz) wurde das BSI-Gesetz um Sicherheitsanforderungen an Kritis-Umgebungen ergänzt, die speziell die Bereiche Energie, Informationstechnik, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen betreffen. Dadurch soll eine Gefährdung der öffentlichen Sicherheit vermieden werden. Kritische Infrastrukturen müssen dabei branchenspezifische Mindeststandards erfüllen, zu denen speziell die Einführung eines Information-Security-Management-Systems (ISMS) zählt. Zusätzlich müssen alle sicherheitsrelevanten Vorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet werden.

Das BSI brachte mit dem IT-Grundschutz im Jahr 2006 ein Konzept für die Umsetzung eines ISMS heraus und bietet Hilfestellungen bei der Einführung und Aufrechterhaltung an. Die Grundschutzkataloge sind inzwischen auch an die internationale Norm ISO/IEC 27001 angepasst, was das Verständnis oder die Erfüllung aber nicht unbedingt erleichtert. Daher stellt ein solches ISMS, das Verfahren und Regeln eines Unternehmens für die IT-Sicherheit definiert, steuert und kontrolliert, eine große Hürde für Unternehmen – speziell für die mittelständischen – dar. Es gibt schlichtweg zu wenig ausreichend ausgebildetes Personal oder entsprechende Ressourcen. So stellen die geforderte Risikoanalyse und das konkrete Auswählen von Maßnahmen viele Firmen vor unlösbare Aufgaben. Aus diesem Grund verzögert sich die ISMS-Einführung oder wurde bisher gar nicht begonnen.

Darüber hinaus ist es auch fraglich, ob das BSI auf die Meldeflut ausreichend vorbereitet ist. Schließlich sollen alle Sicherheitsvorfälle, auch diejenigen ohne Auswirkungen, gemeldet und untersucht werden. Dafür müssten dann beim BSI entsprechende Experten in ausreichendem Maße zur Verfügung stehen und passende Kommunikationsschnittstellen sowie Speichermöglichkeiten angeboten werden.

Das IT-Sicherheitsgesetz legt in jedem Fall fest, dass Betreiber kritischer Infrastrukturen spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, Komponenten oder Prozesse treffen müssen, die für ihre Funktionsfähigkeit maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden, der aber leider nicht definiert wird. Bereits unter IT-Experten wird der Stand der Technik unterschiedlich bewertet bzw. beschrieben. Daher hat ein Kritis-Unternehmen, das nicht im IT-Umfeld agiert, erhebliche Probleme die notwendigen Maßnahmen aus dem IT-Sicherheitsgesetz abzuleiten.

Folgende Aufgaben sind zu erledigen, um konform zum IT-Sicherheitsgesetz zu arbeiten:

- Das Unternehmen muss sich beim BSI registrieren.
- Innerhalb des Unternehmens muss eine Kontaktstelle zum BSI benannt werden.
- Erhebliche IT-Sicherheitsvorfälle müssen dem BSI gemeldet werden.
- Bestimmte Mindeststandards müssen umgesetzt werden, die die eigene IT nach dem Stand der Technik absichern.
- Alle Sicherheitsstandards müssen alle zwei Jahre mittels Audit überprüft werden.

### Kooperationsplattform Disinet

Cyberattacken nehmen kontinuierlich zu. Der letzte große Angriff durch


*Bild 1: Projektwebseite von Disinet (Quelle: www.disi-net.de)*

WannaCry, der als Erpressungstrojaner sein Unwesen im Netz trieb, ist noch allzu gut in Erinnerung. Diese Ransomware verschlüsselte Daten auf den betroffenen Computern, um die Zahlung von Bitcoins zu erpressen. Weltweit sollen 220.000 Systeme betroffen worden sein – die Dunkelziffer liegt sicherlich höher. Anders als sein Vorgänger Locky sprang der Trojaner selbstständig von einem infizierten Rechner auf andere übers Netz erreichbare Windows-Systeme über. Das heißt, der Angriff verband zwei Angriffsvektoren miteinander:

- Infizierung durch den Kryptotrojaner mittels E-Mail;
- Verbreitung durch eine Windows-Lücke als Wurm.

Diese Lücke in der Dateifreigabe (SMB) war durch eine Hackergruppe bereits im Netz vorab bekannt geworden und wurde durch Microsoft in den aktuell unterstützten Betriebssystemen geschlossen. Ältere Windows-Versionen wie XP, die noch im Einsatz waren, konnten aber nicht mehr geschützt werden. Dieses Ereignis macht daher auf zwei Umstände aufmerksam:

- Die Vorgehensweise der Angriffe wird immer intelligenter und kombiniert verschiedene Angriffsvektoren miteinander.
- Es gibt viele Unternehmen (u.a. auch Großkonzerne wie die Deutsche Bahn), die nicht durchgängig mit aktuellen Betriebssystemen arbeiten.

Die Nutzung veralteter Betriebssysteme ist dabei besonders im Produktionsumfeld zu beobachten. Hier wird in ganz anderen Aktualisierungszyklen gedacht: Anlagen und Systeme werden auf den Betrieb für Jahrzehnte ausgelegt und sind nicht für kurze Lebens- und Patch-Zyklen vorgesehen. Das war auch in Ordnung, solange keine Vernetzung oder Anbindung an das Internet durch Industrie-4.0-Lösungen angestrebt wurde. Nun können auf einmal Produktionsrechner über das Internet angesprochen werden, wenn die IT-Sicherheit nicht entsprechend nachgerüstet wird. Die veralteten Systeme sind ein leichtes Ziel, wie WannaCry & Co. gezeigt haben.

Welche Auswirkungen fehlende IT-Sicherheit im Produktionsbetrieb besitzt, kann auch am Beispiel des Internet of Things (IoT, Internet der Dinge) deutlich gemacht werden. Viele Smart-Home-Systeme bieten heute selbstverständlich den Zugriff von außen über die App eines Smartphones an. Dabei haben aber viele Hersteller die IT-Sicherheit zu wenig berücksichtigt, so dass die Systeme teilweise über das Internet sichtbar sind. Über Suchmaschinen wie Shodan kann sogar nach ihnen gesucht werden. Hierüber lassen sich auch Statistiken bekannter Sicherheitslücken wie z.B. Heartbleed abfragen. Dabei ist erkennbar, dass in Deutschland immer noch über 17.000 Systeme bez. Heartbleed nicht aktualisiert wurden. Es wird deutlich, dass auf der einen Seite die Hersteller, aber auch die Betreiber für das Thema IT-Sicherheit noch stärker sensibilisiert werden müssen.

Aus diesem Grund wurde das Kooperationsprojekt Digitalisierung und Sicherheit für Kritische Infrastrukturen (Disinet, **www.disi-net.de**) ins Leben gerufen (*Bild 1*). Dieses im Jahr 2016 neu gegründete Netz will Lösungen für Kritis-Unternehmen anbieten und sie dabei unterstützen, ihre Netz- und Leitsysteme sicher zu betreiben. Dazu sollen Sicherheitsvorfälle vorausschauend erkannt und ihnen entgegengewirkt werden. Ziel von Disinet ist es, sich zu einem Kompetenzzentrum im IT-Sicherheitsbereich, besonders für kleinere und mittlere Unternehmen zu entwickeln. Um dies erreichen zu können, werden aus dem Verbund kleinere Forschungsvorhaben definiert, die sich bestimmten Problemstellungen im Kritis-Umfeld widmen. An dem Kooperationsprojekt sind Industriepartner und Forschungseinrichtungen gleichermaßen beteiligt.

## Monitoring, NAC und SIEM

Das neue IT-Sicherheitsgesetz legt auf zwei Dinge Wert, die Kritis-Unternehmen zukünftig erfüllen müssen: Monitoring (s.a. NET 5/16, S. 33) der IT-Infrastruktur und das Erkennen von Angriffen mittels SIEM (Security Information and Event Management, s.a. NET 10/15, S. 14). Während die erste Variante eigentlich eine Selbstverständlichkeit darstellen sollte, ist man von der vorausschauenden Erkennung noch einen großen Schritt entfernt. Wie notwendig diese ist, kann man an dem neuen Verschlüsselungstrojaner Petya/NotPetya erkennen, der eventuell bereits seit April Daten infiziert, aber noch nicht ausgelöst wurde. Seit diesem Zeitpunkt können sogar Backups kompromittiert worden sein, ohne dass ein Unternehmen bisher davon etwas bemerkt hätte. Das Standardverfahren, das die Kontrolle des eingehenden Netzverkehrs über eine Firewall vorsieht, kann hier nicht mehr als ausreichend bezeichnet werden. Dies sollte zumindest über ein NAC-System (Network Access Control) ergänzt werden. Angriffe oder Bedrohungen werden heute aber so gut wie nicht analysiert. Dies können wiederum SIEM-Systeme leisten.

NAC-Systeme dienen in erster Linie zur Absicherung von Unternehmensnetzen. Immer öfter werden sie auch im Zusammenspiel mit Antiviren-, Intrusion-Detection- (IDS) sowie Intrusion-Prevention-Systemen (IPS) in die IT-Infrastruktur der Unternehmen integriert. Sie haben dabei die Aufgabe, die Benutzer- und Systemauthentifizierung zu kontrollieren. Allerdings fehlt diesen Lösungen der Gesamtüberblick über die IT-Sicherheit im Unternehmen. So werden keine Statistiken über Attacken erfasst, keine kritischen Events generiert, Compliance-Anforderungen überprüft oder ein Risikomanagement durchgeführt. Dies

ist die Domäne von sogenannten SIEM-Systemen, die jedoch relativ kostspielig, personalintensiv und komplex in der Handhabung sind und letztendlich ein weiteres Sicherheitssystem darstellen, das zusätzlich verwaltet werden muss.

Aus diesem Grund wird gerade im BMWI-Forschungsprojekt Clearer (www.clearer-project.de) an einer Architektur gearbeitet, die bestehende NAC-Lösungen mit SIEM-Funktionen ergänzen soll (*Bild 2*). Der Zugang zu einem Unternehmensnetz kann mit NAC dediziert überprüft und ggf. verweigert werden. Das heißt, die wichtigste Aufgabe von NAC ist es, fremde Systeme zu erkennen und nach den Vorgaben der Unternehmensrichtlinien in das Netz zu integrieren oder abzuweisen. Dabei werden Endgeräte während der Phase der Authentifizierung (Authentication) auf Richtlinienkonformität (Policy Compliance) geprüft, um zu gewährleisten, dass nur bekannte und, bezogen auf den Softwarestand, ausreichend aktuelle Endgeräte zugelassen werden. Dies erhöht den Sicherheitsgrad eines Unternehmens enorm.

Über die SIEM-GUI des Clearer-Systems, die als zentrale Oberfläche dient, wird der Systemstatus (Dashboard) angezeigt und eine Compliance-Log-Ansicht ermöglicht. Dadurch können Vorfälle gefiltert und nach Priorität bzw. Dringlichkeit aufgelistet werden. Über ein integriertes Ticketsystem wird der IT-Administrator auf Events aufmerksam gemacht und kann sich über den Status der Bearbeitung informieren. Hinzu kommt, dass Ereignisse miteinander korreliert werden können (Esper), da alle Logs in einer gemeinsamen Datenbank (Apache Cassandra) landen. Das heißt, es müssen nicht mehr alle Logdateien der Sicherheitskomponenten einzeln ausgewertet werden und es sind Querbeziehungen erkennbar, um einen Angriff zusammenhängend identifizieren zu können. Da die zentrale Datenbasis alle Ereignisse des Systems beinhaltet, können Berichte in allen Detailierungsgraden erstellt werden. Ein auf ein Endereignis bezogenes Drill-Down auf die Ursprungsereignisse wird somit möglich. Unterschiedliche Berichte könnten z.B. enthalten, wann welche Komponenten inaktiv waren oder in welchen Zeiten der Compliance-Status verletzt wurde. Auch die Anzahl der Warnmeldungen des Systems in einem bestimmten Zeitraum ließe sich erfassen.

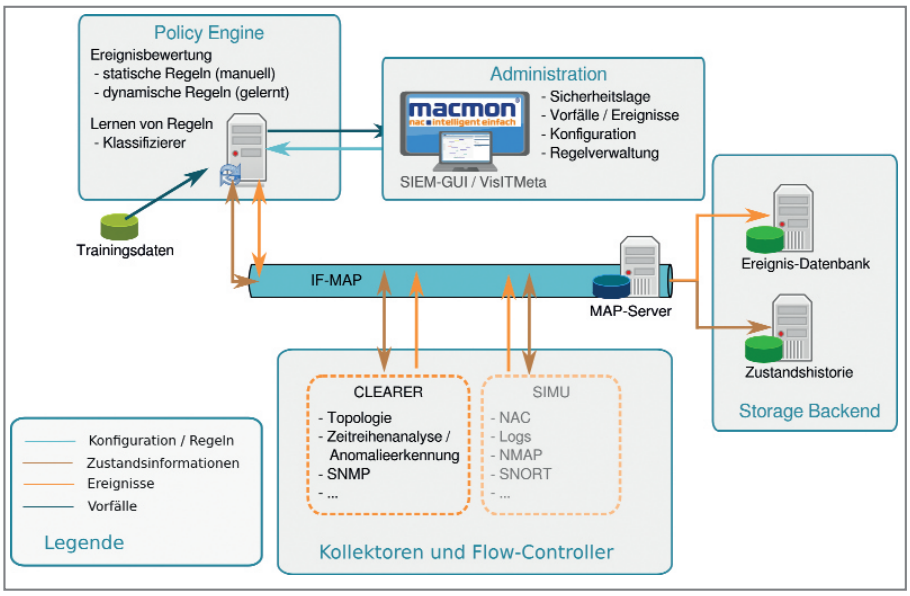


*Bild 2: Generische Architektur von Clearer*

In Produktionsumgebungen lassen sich solche Lösungen allerdings nicht ohne weiteres integrieren, da sie andere Anforderungen besitzen als im Büroumfeld. So kann ein aktiver Scan des Netzes bereits zu Problemen führen, wenn CPU-schwache Systeme in Produktionsanlagen überwacht werden sollen. Die Verfügbarkeit steht in Produktionsnetzen weit über allen anderen Anforderungen und darf nicht durch zusätzliche IT-Sicherheitsmechanismen beeinträchtigt werden. Es wird daher noch viel an Industrie-4.0-Szenarien gearbeitet, da hier die Vernetzung zwingend erforderlich ist, aber neue Sicherheitslücken aufgerissen werden.

## Fazit

Die Bereiche Vertraulichkeit, Integrität und Verfügbarkeit von Informationen werden für Unternehmen immer wichtiger, um ihrem normalen Tagesgeschäft nachgehen zu können. Die Angriffswellen treten in immer kürzeren Abständen auf und werden immer intelligenter. Zusätzlich werden neue Gesetze, wie das IT-Sicherheitsgesetz, auf den Weg gebracht, die speziell Unternehmen mit Kritis-Umgebung zur Erhöhung ihrer bestehenden Sicherheitsplattformen zwingen sollen. Das scheint auch notwendig zu sein, da viele Kritis-Betreiber (Stadtwerke, Energieversorger, Kläranlagenbetreiber usw.) erst nach der Einführung des IT-Sicherheitsgesetzes angefangen haben zu reagieren. Allerdings ruderte der Gesetzgeber auch wieder etwas zurück, da er nachträglich den Regelschwellwert auf 500.000 zu versorgende Personen festgelegt hat. Andere Betreiber sind von der Regelung daher wieder ausgeschlossen. Durch die Vernetzung der Betreiber werden Schwachstellen in kleineren Betrieben in Kauf genommen, die als Angriffsvektoren von Hackern genutzt werden können.

Was ein Ausfall kritischer Infrastrukturen bewirken kann, wurde in dem Roman „Blackout" von Marc Elsberg eindrucksvoll gezeigt. Hier war durch einen Stromausfall, der durch einen Hacking-Angriff eines Smart-Grid-Gerätes ausgelöst wurde, die gesamte Zivilisation betroffen. Bei der Absicherung von Kritis-Betreibern geht es nicht mehr nur um einen Ausfall einzelner Unternehmen, sondern um die Gesamtabsicherung kritischer Systeme, deren Ausfall weitreichende Folgen haben könnte. Daher sollten alle Betreiber, unabhängig von Gesetzgebung und Größe, Interesse an der Erhöhung ihrer Sicherheitsstandards haben. *(bk)*