Kompetenzreihe

Dem IT-Sicherheitsgesetz einen Schritt voraus

Was Betreiber kritischer Infrastrukturen schon heute für den faktischen Schutz vor Cyberangriffen tun können

IT Security
made in Europe

RADAR SERVICES

Hintergrund

Die Digitalisierung bietet große Chancen, zugleich aber auch eine große Angriffsfläche für Cyberattacken mit weitreichenden Folgen. Vor diesem Hintergrund stellt eine **vorausschauende Sicherheitspolitik für den Schutz der IT von bedeutenden Infrastrukturbetreibern** eine zentrale Aufgabe eines Landes dar. Um den IT-Standort Deutschland langfristig abzusichern, ist das IT-Sicherheitsgesetz in Deutschland am 25. Juli 2015 in Kraft getreten. Erklärtes Ziel des Gesetzgebers ist es, die Sicherheit informationstechnischer Systeme zu erhöhen.

Aus faktischer Sicht sind die zukünftig gesetzlich geforderten Maßnahmen für das Funktionieren des täglichen Lebens von Millionen Menschen wichtig. Was passiert, wenn großflächig der Strom ausfällt? Was, wenn in Krankenhäusern falsche Daten bei der Patientenbetreuung verarbeitet werden? Was, wenn die Wasserversorgung in ganzen Landkreisen stockt?

Die Bereiche der kritischen Infrastruktur

In erster Linie zielt das neue IT-Sicherheitsgesetz auf Unternehmen ab, die als Betreiber sogenannter „Kritischer Infrastrukturen“ – abgekürzt **„KRITIS“** – betrachtet werden. Als kritische Infrastrukturen werden jene IT-Systeme bezeichnet, deren Ausfall bzw. Beeinträchtigung ernsthafte Versorgungsengpässe, drastische Störungen der öffentlichen Sicherheit oder andere schwerwiegende Folgen für das Gemeinwohl des Staates und seiner Bürger haben würden. Im Zentrum dieser gesetzlichen Neuregelung stehen insbesondere **Unternehmen aus den Bereichen Energie, Ernährung, Gesundheit, Wasser, Transporte & Verkehr, IT und Telekommunikation sowie das Finanz- und Versicherungswesen**.

Das Bundesministerium für Inneres erarbeitet derzeit eine Rechtsverordnung, die eine konkrete Definition der „KRITIS“-Unternehmen umfasst. Ausgenommen sind nach derzeitigem Stand Kleinstunternehmen, d.h. Firmen mit weniger als 10 Mitarbeitern und weniger als 2 Millionen Euro Jahresumsatz.

Die Forderungen des IT-Sicherheitsgesetzes

„KRITIS"-Unternehmen werden durch das IT-Sicherheitsgesetz verpflichtet, bestimmte **Mindeststandards für die Sicherheit ihrer IT-Infrastruktur** zu etablieren. Sie werden gefordert, **organisatorische und technische Vorkehrungen** zu treffen, um eine Störung der informationstechnischen Systeme, Komponenten oder Prozesse zu vermeiden, welche wiederum die Funktionsfähigkeit der betriebenen kritischen Infrastrukturen sicherstellen. Zusätzlich sollen die jeweiligen Branchen auch selbst Standards entwickeln, die folglich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) abgesegnet werden.

Laut IT-Sicherheitsgesetz müssen die erwähnten Sicherheitsmaßnahmen „**angemessen**" sein und dem „**Stand der Technik**" entsprechen. Unter Angemessenheit versteht man in diesem Fall, dass der erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen „KRITIS" stehen soll.

Getroffene Maßnahmen sind von den Betreibern in Sicherheits- und Notfallkonzepten festzuhalten, deren Umsetzung ist zu dokumentieren. Zudem müssen KRITIS-Unternehmen im Rahmen der **Prävention** im Zwei-Jahres-Rhythmus ihre Sicherheitsmaßnahmen prüfen lassen und mittels Audits oder Zertifizierungen nachweisen. Ergebnisse sind an das BSI zu melden. Bereits etablierte Standards für Informationssicherheit wie die ISO/IEC 27000-Familie oder der BSI Grundschutz können bei der Umsetzung von Unternehmen angewandt werden. Für die laufende Kommunikation mit dem BSI sind Kommunikationsstellen in den jeweiligen Unternehmen zu definieren.

Das IT-Sicherheitsgesetz sieht auch **Meldepflichten** bei IT-Sicherheitsvorfällen vor. In der Regel erfolgen sie anonym, sollte es jedoch der Fall sein, dass ein vollständiger Systemausfall droht, so muss auch der Name des Unternehmens an das BSI gemeldet werden. Laut Schätzungen der deutschen Regierung wird die Meldepflicht **etwa 2.000 Unternehmen** betreffen.

Für Betreiber von Webservern gelten bereits ab Inkrafttreten des IT-Sicherheitsgesetzes am 25. Juli 2015 erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme. Darüber hinaus gelten für Betreiber von Kernkraftwerken und Telekommunikationsunternehmen ebenfalls bereits seit Inkrafttreten neue Pflichten zur Meldung von erheblichen IT-Sicherheitsvorfällen. Für sonstige KRITIS-Unternehmen gilt eine entsprechende Meldepflicht nach Inkrafttreten der das IT-Sicherheitsgesetz konkretisierenden Rechtsverordnung.

Im Fall einer Nicht-Beachtung von Sicherheitsanforderungen bzw. eine Nicht-Meldung muss mit **Strafen** von bis zu 100.000 Euro gerechnet werden.

Die Agenda auf EU-Ebene

Cyberangriffe zu bekämpfen und die Netzwerk- und Informationssicherheit zu erhöhen sind Ziele, die auch auf der Agenda der Europäischen Union weit oben gereiht sind. Das Hauptziel der EU-Cybersicherheitsstrategie ist die **Prävention von und Reaktion auf Cyberangriffe**. Bereits 2004 wurde durch die Gründung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) ein Schritt in die Richtung der Umsetzung dieser Ziele gesetzt. Seit 2013 wird an der EU-Richtlinie zur Cybersicherheit gearbeitet.

Eine wesentliche Maßnahme ist auch die geplante **Richtlinie für Netz- und Informationssicherheit** (network and information security – NIS). So soll in dieser Richtlinie festgelegt werden, dass alle Mitgliedstaaten der EU, wichtige Internetfirmen und Infrastrukturbetreiber, E-Commerce Plattformen, soziale Netze sowie Anbieter von Dienstleistungen im Verkehrsbereich, im Bankgeschäft und im Gesundheitswesen ein sicheres und vertrauenswürdiges digitales Umfeld gewährleisten. Die genannten Bereiche ähneln stark den durch das IT-Sicherheitsgesetz festgelegten „Kritischen Infrastrukturen", wobei die deutsche Gesetzgebung im Gegenzug zur geplanten EU-Richtlinie auch die Sektoren Wasser und Ernährung miteinbezieht.

Wie auf deutscher Ebene sind **Meldepflichten** für IT-Vorfälle vorgesehen. Ende des Jahres 2015 wurde der gemeinsame Entwurf von EU-Kommission, EU-Rat und EU-Parlament vorgelegt. Wann die NIS-Richtlinie tatsächlich in Kraft treten wird, ist aktuell noch nicht absehbar.

Dem IT-Sicherheitsgesetz einen Schritt voraus:

was kritische Infrastrukturbetreiber schon heute für den faktischen Schutz vor Cyberangriffen tun können

Das IT-Sicherheitsgesetz verlangt von Unternehmen, die zentral für das Funktionieren des täglichen Lebens von Millionen Menschen sind, Maßnahmen zum laufenden Schutz ihrer IT vor Angriffen.

Einzelmaßnahmen werden im Gesetz nicht konkret vorgeschrieben. Die Forderung von dem „Stand der Technik" entsprechenden Maßnahmen ist aus heutiger Sicht jedoch klar in eine Richtung zu verstehen:

Herkömmliche Sicherheitsmechanismen – vom Virenschutz über die Firewall bis zur Netzwerküberwachungssoftware – sind notwendig, sie bieten aber keinen ausreichenden Schutz. Sie decken alle ihre jeweiligen, ganz speziellen Einsatzgebiete ab und arbeiten nebeneinander, nicht zusammen und nicht als selbstlernende Systeme. Sie werden von professionellen Angreifern mit wenig Aufwand überlistet.

State of the Art ist vielmehr die Einrichtung eines **dauerhaften Schutzschirmes, der über dem Unternehmensnetzwerk aufgespannt wird und alle Erkenntnisse der beteiligten Systeme analysiert**. Isolierte Ereignisse, die für sich unverdächtig erscheinen, deuten als Teil eines Gesamtbildes auf einen Angriff hin und müssen genauso betrachtet werden.

„KRITIS"-Unternehmen müssen ihren **Fokus also auf das proaktive Aufspüren von Sicherheitslücken und das zeitnahe Erkennen von Angriffen auf Ihre IT** statt auf die Abwehr „fiktiver" Gefahren richten. Diese Herangehensweise ist die einzige Möglichkeit, den Schaden für Kunden/Verbraucher und das eigene Unternehmen im Angriffsfall zu begrenzen.

Die Etablierung eines umfassenden IT Security Monitorings heißt dabei nicht, neue Tools neben alte zu stellen. Tatsächlicher Schutz wird nur erzielt, wenn die **Funktionsweisen und Ergebnisse der verschiedenen Monitoring-Programme laufend von Experten analysiert, die Konfiguration durchgehend an aktuelle Gegebenheiten angepasst und die Programme an sich ständig weiterentwickelt** werden. Die Ressource Mensch kann also in der IT-Sicherheit bis heute durch kein Programm ersetzt werden.

Die kontinuierliche Gesamtüberprüfung der IT-Infrastruktur durch Mensch und Technik liefert alle notwendigen Informationen, um potentiellen Schaden von Angriffen bestmöglich zu minimieren. Sie umfasst drei Komponenten: eine kontinuierliche Schwachstellenanalysen von innen und außen, eine laufende Analyse und Korrelation von Logs der einzelnen Systeme und eine ständige Überwachung aller Einfallstore für Schadsoftware und aller Kommunikationskanäle über die Unternehmensgrenzen hinweg.

Die kontinuierliche Schwachstellenanalyse

Jeden Tag versuchen Angreifer noch nicht bekannte Sicherheitslücken oder Schwachstellen in der IT eines Unternehmens aufzufinden. Das kontinuierliche Aufspüren dieser Probleme aus einer **internen Sicht (innerhalb des Unternehmensnetzwerkes) und aus einer externen (aus dem Internet)** ist Voraussetzung, um zum Beispiel fehlende oder unsichere Verschlüsselung aufzudecken.

Die Log-Datenanalyse und Korrelation

Angreifer versuchen ihre Bewegungen im Netzwerk so normal wie möglich aussehen zu lassen. Dennoch könnten zum Beispiel Logins von einem Benutzer auf mehreren Systemen von unterschiedlichen IPs zur gleichen Zeit verdächtig sein. **Alle Logs von Servern, Netzwerkgeräten, Applikationen und anderen zentralen Einrichtungen** müssen daher **zentral analysiert und** mit den Erkenntnissen aus Intrusion Detection Systemen (IDS) **korreliert** werden.

Die Überwachung der Einfallstore für Schadsoftware und der Kommunikationskanäle

Ein Angreifer wird früher oder später Daten aus dem Unternehmen zu externen Zielen im Internet übertragen. Dies fällt bei einem umfangreichen **Security Monitoring aller Systeme, des Datenverkehrs und der Zugriffe auf sensible Systeme und Dateien** auf. Datentransfer von internen zu externen IPs, zu denen keine Geschäftsbeziehung besteht, muss umgehend festgestellt und von Experten analysiert werden. Dies erfordert den Einsatz von **Intrusion Detection Systemen (IDS)** und anderen Werkzeugen sowie die Unterstützung durch Experten, die diese richtig konfigurieren, an aktuelle Gegebenheiten anpassen und deren Erkenntnisse analysieren.

Das zentrale Ziel: die Verkürzung der Zeit zwischen Angriff und seiner Entdeckung

Eine **proaktive Sicherheitsstrategie** mit lückenlosem Monitoring und kontinuierlicher Analyse verkürzt die Zeitspanne zwischen Angriff und Entdeckung drastisch. Jeglicher Schaden, sei es Schaden durch eine Leistungsunterbrechung oder -stillstand, durch Entwendung von Kundendaten oder andere Beeinträchtigungen wird so am effektivsten minimiert.

Die proaktive Sicherheitsstrategie konzeptionieren

Wichtig ist, dass in das lückenlose Monitoring und die kontinuierliche Analyse möglichst **die gesamte IT-Infrastruktur**, einschließlich der Applikationsebene, **in eine fortlaufende, kontextbezogene Überwachung in Echtzeit einbezogen wird**. Sämtliche potenziell risikorelevanten Informationen, sowohl bezogen auf den Status von IT Systemen (z.B. Schwachstellen) als auch bezüglich des Verhaltens von IT-Systemen (z.B. Netzwerkdatenverkehr) müssen dafür gesammelt und verarbeitet werden. In der Folge ist es erforderlich, diese Flut an gespeicherten risikorelevanten Informationen auf die tatsächlich bedeutsamen Ereignisse zu verdichten. **Die Qualität dieser Verdichtung hängt dabei einerseits maßgeblich von der Ausrichtung und Funktionalität des vorhandenen Korrelationssystems ab. Andererseits ist es entscheidend, umfassende Risikoerkennungsszenarien abzubilden**, um selbst komplexe Muster von Cyberangriffen zu erkennen.

Blinde Flecken schaffen Risiken

Moderne IT Systeme sind hochgradig vernetzt und voneinander abhängig. Mit dem Integrationsgrad der IT-Umgebungen steigt jedoch auch das Risiko, da das schwächste Glied der Systemkette oftmals Ausgangspunkt für Cyberattacken ist. Es ist daher entscheidend, eine **möglichst umfassende Analysetiefe** zu erzeugen. Das bedeutet, dass der Schwachstellenzustand sämtlicher IT-Systeme und Applikationen, der gesamte interne Netzwerkdaten- sowie der Internetdatenverkehr bei sämtlichen Internetzugängen als auch Verhaltensinformationen aller relevanten IT-Systeme (d.h. Log-Daten von Systemen und Applikationen) kontinuierlich betrachtet werden müssen. Konfigurationsänderungen auf IT-Systemen sollten ebenso berücksichtigt werden wie unerlaubte oder unerwünschte Software, die darauf läuft. Laufend aktualisierte Inventar- und Konfigurationsübersichten sind notwendig, um korrekte Risikobehebungsmaßnahmen ableiten zu können. Eingehende Dokumente und Emails sollten mit modernsten Sandboxingtechnologien analysiert werden.

Die Herausforderung „Advanced Cyber Attacks“

Nicht jede Cyberattacke kann anhand statischer Erkennungsregeln erkannt werden. Bei neuen Generationen von Cyberattacken ist es erforderlich, zunehmend verhaltensorientierte Analysemethoden einzubeziehen. Das „IT-Frühwarnsystem“ benötigt dafür „**Advanced Correlation Engines**“ oder auch „**Behavioral Analysis Systems**“. Diese Systeme müssen für eine eingehende Analyse von „Advanced Cyber Attacks“ in der Lage sein durch die Anwendung statistischer Modelle, rekursiver Methoden und selbstlernender Algorithmen zwischen normalem und abnormalem Verhalten von IT-Systemen zu unterscheiden. Somit bieten modernste Erkennungssysteme erstmals effektive Methoden, um auch komplexe Cyberattacken, deren Durchführung mitunter Wochen oder Monate in Anspruch nimmt und eine Vielzahl unterschiedlicher Systeme betrifft, zu erkennen.

Qualität und Effizienz bei der Umsetzung der geforderten Maßnahmen

Das komplette Set dieser hochspezialisierten Analysen basierend auf Mensch und Technik wird ressourcenschonend vom europäischen Managed Security Services Anbieter **RadarServices** erbracht. Die Dienstleistungen **kombinieren die automatisierte Erkennung von IT-Sicherheitsproblemen und -risiken im ersten Schritt mit der Analyse durch hochspezialisierte IT-Sicherheitsexperten im zweiten Schritt**. Die Besonderheit von RadarServices liegt dabei darin, dass **Daten während des gesamten Prozesses nie das Kundenunternehmen verlassen**, womit ein einzigartig hoher Standard an Vertraulichkeit und Sicherheit gewährleistet wird.

Beim Einsatz von RadarServices wird auch die Umsetzung der vom Gesetzgeber festgeschriebenen „**Angemessenheit**“ der Sicherheitsmaßnahmen durch hocheffiziente Strukturen im IT-Sicherheitsmanagement unterstützt. **Für die Einrichtung, Konfiguration und den täglichen Betrieb sind keine zusätzlichen personellen oder finanziellen Ressourcen notwendig**. Im Vergleich zu einer Inhouse-Lösung ergeben sich so zentrale Vorteile: **langfristige Investitionsrisiken**, die bei einer Inhouse-Lösung aus der Anschaffung von umfangreich benötigter Hard- und Software sowie aus dem Aufbau und der kontinuierlichen Weiterbildung eines stetig wachsenden Teams an hochspezialisierten Experten resultieren, werden **drastisch reduziert**.

Durch die Arbeit von RadarServices bekommen IT-Teams im Kundenunternehmen **konsolidierte und verifizierte IT-Risiko- und Sicherheitsinformationen**, die sofort **für den Behebungsprozess** verwendbar sind. Sie können sich damit vollkommen auf die umgehende Behebung konzentrieren und werden auf Wunsch auch

hierbei unterstützt, sei es durch „Fire Fighting“, der Hilfe bei akuten Problemen oder auch bei operativen oder strategischen Aufgaben im gesamten IT-Sicherheitsmanagement.

Zusammenfassung

Das IT-Sicherheitsgesetz setzt einen branchenübergreifenden Startpunkt des Gesetzgebers, Unternehmen, deren Ausfall bzw. Beeinträchtigung ernsthafte Versorgungsengpässe, drastische Störungen der öffentlichen Sicherheit oder andere schwerwiegende Folgen für das Gemeinwohl des Staates und seiner Bürger haben würden, zu umfassenden IT-Sicherheitsmaßnahmen anzuhalten. Vorstöße in die gleiche Richtung werden auf EU-Ebene forciert.

Bei allen Initiativen werden den Unternehmen Spielräume für die für sie konkret passenden IT-Sicherheitsmaßnahmen gegeben. Der Grundtenor, der sich durch die Forderung von Maßnahmen nach dem „Stand der Technik“ ausdrückt, scheint jedoch schon heute eindeutig: „herkömmliche“ Sicherheitsmechanismen – vom Virenschutz über die Firewall bis zur Netzwerküberwachungssoftware – bieten keinen ausreichenden Schutz. State of the Art ist das **proaktive Aufspüren von Sicherheitslücken und das zeitnahe Erkennen von Angriffen auf die IT statt die Abwehr „fiktiver“ Gefahren**. Ein lückenloses IT Security Monitoring und eine kontinuierliche Schwachstellenanalyse verkürzen die Zeitspanne zwischen Angriff und Entdeckung drastisch und minimieren potentiellen Schaden am effektivsten.

Höchste Qualitäts- und Effizienzansprüche werden bei der Umsetzung der geforderten Maßnahmen unter Einbeziehung von Managed Security Services erzielt. **RadarServices**, Europas führender Anbieter für IT Security Monitoring und IT Risk Detection als Managed Services, bietet den **kompletten Werkzeugkasten und den Zugriff auf die benötigten hochspezialisierten Experten** aus einer Hand.

Ihr Ansprechpartner bei RadarServices

Dr. Isabell Claus
Head of Corporate Affairs

RadarServices
Hasnerstraße 123, 1160 Wien
Österreich

T: +43 (1) 929 12 71-33
isabell.claus@radarservices.com

RadarServices ist Europas führender Anbieter von Managed Security Services. Im Mittelpunkt steht die zeitnahe Erkennung von IT-Sicherheitsrisiken. Daten verlassen dabei niemals ein Kundenunternehmen. Die Services kombinieren (1) die in Europa entwickelte Technologie, (2) die Arbeit der Analyseexperten in den weltweiten Security Operations Centers (SOCs) und (3) bewährte Prozesse und Best Practices bei IT-Sicherheitsvorfällen. Das Ergebnis: Eine besonders effektive und effiziente Verbesserung von IT-Sicherheit und Risikomanagement, ein kontinuierliches IT Security Monitoring und ein auf Knopfdruck verfügbarer Überblick über die sicherheitsrelevanten Informationen im Gesamtunternehmen.

RadarServices
Zieglergasse 6
1070 Wien
Österreich

T: +43 (1) 929 12 71-0
F: +43 (1) 929 12 71-710
E: sales@radarservices.com
www.radarservices.com

RadarServices Deutschland
Taunustor 1
60310 Frankfurt a. M.

T: +49 (69) 2443424 655
E: sales_germany@radarservices.com

RadarServices Middle East
A110-1, DSO HQ Building
Dubai, VAE

T: +971 (4) 501 5447
E: sales_me@radarservices.com

Detecting Risk,
Protecting Value