Sonderdruck 2016 Oktober

IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Compliance

Sonderdruck für bridging IT Menschen Methoden Lösungen

Planvoll vom perimetergestützten Grundschutz zur Cyber-Security mit Augenmaß

Nicht mehr als notwendig und leistbar

Mit der Hinwendung der Unternehmen zum Digital Business delegieren sie Teile ihrer IT-Infrastruktur und IT-Services an Cloud-Provider. Damit übertragen sie für diese Teile auch die Sicherheitsvorkehrungen und -maßnahmen an diese Dienstleister. Wird diese Delegation nicht durch geeignete Techniken und Maßnahmen für Cyber-Security sowie zum Management digitaler Restrisiken flankiert, parallel die eigenen IT-Infrastruktur verlässlich geschützt, drohen den Unternehmen Serviceausfälle und inakzeptable Sicherheitseinbußen.

Nach einem aktuellen Spezialreport von Gartner, „Cybersecurity at the Speed of Digital Business", werden 2020 60 Prozent der digitalen Geschäftsauftritte mit gravierenden Serviceausfällen konfrontiert sein, wenn die Unternehmen weder die Sicherheitswerkzeuge noch die Sicherheitsteams auf Cyber-Security und das Management digitaler (Geschäfts-)Risiken abstimmen. Mit dem Digital Business geht in den Unternehmen sowohl eine technische als auch organisatorische digitale Transformation einher. Demzufolge stellt Cyber-Security und das Management der mit den digitalen Geschäften verbundenen Risiken für Unternehmen eine technische und organisatorische Herausforderung dar. Allerdings warnt Paul Proctor, Vice President und Analyst bei Gartner, die Unternehmen vor übertriebenen Erwartungen. Die Unternehmen müssten mit ihrem Engagement im Cyberspace lernen, mit akzeptablen digitalen Sicherheitsrisiken zu leben. Und sie müssten herausfinden und differenzieren, welches Maß an Sicherheit und Risikomanagement sie brauchen und für sie leistbar ist.

Fünf Handlungsschlüsselfelder

Gartner hat ausgehend von der unternehmenseigenen IT-Infrastruktur fünf Handlungsschlüsselfelder für Cyber-Security und das Management von Risiken im digitalen Geschäftsumfeld identifiziert:

- Kontrolle und Governance ausbauen,
- gefährliche Ereignisse und Verhaltensweisen schnell erkennen und dafür geeignete

Abwehrtechniken und -maßnahmen etablieren beziehungsweise herausbilden,
- Strategien zur Informationssicherheit und Risikokontrolle der hohen Geschwindigkeit der digitalen Geschäfte anpassen,
- in diese Strategien die Cloud Provider einbinden, die zunehmend IT-Service- und Sicherheitsaufgaben übernehmen werden, wobei weiterhin das Unternehmen für die Einhaltung vereinbarter IT-Service- und Sicherheits-Levels sowie IT-Compliance und -Governance verantwortlich zeichnet,
- digitale Arbeits- und Verhaltensweisen sowohl der eigenen Mitarbeiter als auch des Personals bei Cloud-Providern bei der Herausbildung von Cyber-Security berücksichtigen, beispielsweise durch eine benutzerzentrische Kontrolle der Zugriffe.

Dabei gilt es, alle fünf Handlungsschlüsselfelder ganzheitlich zu betrachten und zu projektieren, damit später alle Sicherheitswerkzeuge und -maßnahmen sowie die Kontrolle maßgeblicher Restrisiken nahtlos ineinanderwirken.

Risikoanalyse muss sein

Um gefährliche Ereignisse und Verhaltensweisen aus dem Cyberspace erkennen und hinsichtlich ihrer potenziellen Auswirkungen auf die IT-Infrastruktur, die IT-Servicebereitstellung und die digitalen Geschäftsprozesse bewerten zu können, führt für das Unternehmen kein Weg an einer gründlichen Risikoanalyse vorbei. Je geschäftskritischer die Daten, Anwendungen, IT-Services und Geschäftsprozesse für das Unternehmen sind, umso besser sollten sie durch geeignete Techniken und Maßnahmen für Cyber-Security geschützt und umso lückenloser sollten später gefährliche Restrisiken permanent überwacht und kontrolliert werden. Für eine abschließende Risikobewertung muss das Unternehmen außerdem wissen, in welchem Kontext Datenbestände, Anwendungen, Server, IT-Services, Geschäftsprozessen sowie die Benutzer, die daran mitwirken, stehen. In diese kontextuellen Betrachtungen müssen auch die bei den Cloud-Providern angesiedelten IT-Ressourcen, IT-Services, Geschäftsprozesse und Unterstützungskräfte einbezogen werden. Für diese eingehende und umfassende Risikoanalyse und -bewertung sprechen viele gute Gründe. Nur mit diesem Wissen:

- können Sicherheitsrisiken mit hohem Gefahrenpotenzial von akzeptablen Risiken unterschieden werden.
- können gezielt geeignete Sicherheitswerkzeuge und -maßnahmen eingesetzt beziehungsweise etabliert werden.
- kann später die Verfolgung und Behebung der Restrisiken je nach Dringlichkeit priorisiert werden.
- können Cloud-Provider gezielt mit Sicherheits-, Überwachungs- und Behebungsaufgaben betraut werden.
- kann die Qualität der externen Sicherheitsdienste kontrolliert und bewertet und deren Ausführung für IT-Compliance und -Governance allgemein verbindlich dokumentiert werden.
- können Cloud-Provider in die Cyber-Security-Strategie des Unternehmens eingebunden und gemäß dieser Strategie überwacht und gesteuert werden.

Assessment des Grundschutzniveaus

Für die Auswahl geeigneter Sicherheitswerkzeuge und die Etablierung angemessener Sicherheitsmaßnahmen muss das Unternehmen außerdem den Status quo der internen Sicherheitsvorkehrungen, das Grundschutzniveau, genau kennen/ermitteln (Assess-

Auswahl an Cyber-Security-Werkzeugen:

- Perimeter- und Endpunkt-Sicherheit
- Identity and Access Management
- Sicherheit der mobilen Geräte (Hard-/Software)
- Intrusion Detection/Prevention Monitoring
- Abwehr von Advanced Persistent Threats (APTs)
- Event-Überwachung und -Korrelation/Analytics
  Vulnerability Testing
- Penetration Testing
- Security Intelligence
- Verschlüsselungslösungen
- sichere E-Mail-Lösungen

ment). Nur unter dieser Voraussetzung wird es auf den bisher Perimeter-basierenden Sicherheitstechniken gezielt mit Cyber-Security-Techniken aufbauen können, um damit und mit den Ergebnissen der Risikoanalyse die wichtigsten Flanken zu decken (Ziel). Zu einem verlässlichen Grundschutz gehört, dass klassische Techniken wie Firewalls oder Virenscanner per Update immer auf dem aktuellen Stand sind. Unified Threat Management und die Vergabe von Zugriffsberechtigungen sollten zentral erfolgen. Sensible Datenströme einschließlich ein- und ausgehender E-Mails sollten stark verschlüsselt werden, außerdem durch Anti-Spam-Schutz flankiert werden. Mobile Endgeräte ebenso wie die darauf befindlichen IT-Ressourcen und Funktionen sollten physisch und logisch gegen Missbrauch geschützt sein. Penetrationstests unterstützen darin, potenzielle Schwachstellen innerhalb des Grundschutzes ausfindig zu machen.

Vielfältige neue Bedrohungen

Die Gefahren aus dem Cyberspace, denen nicht mit den perimetergestützten Sicherheitstechniken des Grundschutzes Paroli geboten werden kann, sind vielfältig:

- Kampagnen, die auf Vektoren aufsetzen und auf die Klick-Bereitschaft der Benutzer bauen,
- Angriffe über Standard-Malware-Tools, die leicht über das Internet bezogen werden können,
- Standard-Werkzeuge, die sich Advanced-Persistent-Threats (APT)-Methoden zunutze machen,
- Advanced-Threat-Kampagnen, um Anmeldedaten von Benutzern abzugreifen,
- Massenkampagnen ebenfalls mit Zielrichtung Benutzer, um sich beispielsweise über einen URL-basierenden Vektor und mittels Traffic-Direction-Systemen (TDS) oder Exploit-Kits Kerndaten und Payloads anzueignen,
- in offiziellen App-Stores eingeschleuste Malware, um sie, vorerst unentdeckt, in die IT-Infrastruktur des Unternehmens zu infiltrieren, danach darüber Kerndaten, Login- und Anmeldedaten auszuspähen,
- Infiltration von Malware über Social-Media-Konten, um darüber sensible Daten abzuziehen oder durch Fremdsteuerung Einfluss zu nehmen und Aktivitäten zu übernehmen,
- Erschleichen von Zugriffsrechten, allen voran Rechte von Schlüsselpersonen.

Cyber-Security mit Augenmaß

Die richtige Auswahl an Werkzeugen zu treffen, um basierend auf dem Grundschutz Cyber-Security mit Augenmaß gemäß den Ergebnissen der Risikoanalyse zu errichten, ist nicht einfach. Die Unternehmen werden in einem überhitzten Sicherheitsmarkt förmlich mit unzähligen Cyber-Security-Werkzeugen bombardiert, die für den Einsatz mehr oder weniger sinnvoll sind. Welche dieser Werkzeuge tatsächlich gebraucht werden, ist sowohl vom etablierten Grundschutzniveau als auch von den gesetzten Zielen – welche Sicherheits- und digitalen Risiken müssen weitgehend ausgeschlossen werden, welche können hingegen toleriert werden – abhängig. Aber nicht nur die Art der Werkzeuge will bei der Auswahl bedacht sein. Mit in die Produktentscheidung einfließen sollten weitere Kriterien wie die Ausrichtung, funktionale Abdeckung, Herkunft, Anschaffungskosten, Betriebs- und Weiterentwicklungskosten ebenso mögliche funktionale Überschneidungen oder Unverträglichkeiten zwischen unterschiedlichen Werkzeugen.

Awareness sicherstellen

Nicht vergessen werden sollte auf dem Weg zu Cyber-Security mit Augenmaß die Durchführung von internen Awareness-Programmen. Sie sollten sich aus Schulungen und Marketingaktionen zusammensetzen. Als Werkzeuge zur Sensibilisierung der Mitarbeiter können E-Learning, Awareness-Kampagnen und Flyer herangezogen werden. Solche internen Awareness-Programme sind notwendig, um in Zeiten der Abwehr von immer intelligenteren Attacken aus dem Cyberspace nicht nur intern, sondern unterstützend auch extern bei den Cloud-Providern das notwendige Sicherheitsbewusstsein aufzubauen, danach zu pflegen und zu erhalten.

Eines steht außer Frage, trotz aller Sicherheitsvorkehrungen: Externe Cloud-Betriebsmodelle, um darüber den digitalen Geschäftsauftritt voranzutreiben, sind für ein Unternehmen fast immer mit Sicherheitseinbußen verbunden. Treten gefährliche Ereignisse oder Verhaltensweisen auf, muss es sich auf die Qualität der Überwachung und Eingriffe sowie die Informationspolitik der Cloud-Provider verlassen können. Diese Erwartungshaltung kann mit der internen Betriebspolitik des Cloud-Providers – Kostenerwägungen, mangelnde Transparenz, beispielsweise um Imageschäden oder Strafzahlungen zu vermeiden – kollidieren. So verzichtet das Unternehmen mit der Inanspruchnahme externer Cloud-Betriebsmodelle beim Auftreten gefährlicher Ereignisse und Verhaltensweisen darauf, direkt korrigierend eingreifen und Gegenmaßnahmen einleiten zu können. Mit der Übertragung an die Cloud-Provider verlassen die Daten zudem das sicherere Corporate Network und werden dadurch während des Transports anfälliger für Angriffe, die von überall aus dem Internet von Hackern oder Industriespionen ausgehen. Dennoch steht das Unternehmen weiterhin auch für die übertragenen und extern gespeicherten und verarbeiteten Daten und Kundendaten in der Pflicht, Stichworte: IT-Compliance und -Governance. ■

CARSTEN TRIEBEL,
Senior Consultant
beim Beratungsunternehmen bridgingIT