HWB
Handelsverband
Wohnen und Büro

IT Sicherheit: Die wesentlichen Eckpunkte, die laut BSI zu befolgen sind

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet als nationale Cyber-Sicherheitsbehörde kontinuierlich die Gefährdungslage der IT-Sicherheit in Deutschland. Im Fokus des BSI stehen Cyber-Angriffe auf Unternehmen, staatliche sowie öffentliche Institutionen und Privatpersonen, aber auch Maßnahmen zur Prävention und Bekämpfung dieser Lagen.
Es werden folgende Empfehlungen durch das BSI gegeben:

- Die wichtigste Voraussetzung für die Wiederherstellung der Betriebsfähigkeit nach einem Ransomware-Angriff ist eine klare Backup-Strategie. Diese umfasst die Verfügbarkeit funktionierender und aktueller Backups.
  Die Funktionsfähigkeit dieser Backups muss regelmäßig geprüft werden. Es ist inzwischen bei Schadprogramm-Infektionen üblich, dass Angreifende mit zuvor erlangten Administrationsrechten gezielt nach allen Backups suchen und diese, ebenso wie Produktivsysteme, verschlüsseln. Daher sollte zumindest je eine Kopie offline gesichert werden. Diese Kopien werden nach dem Backup von den anderen Systemen der Einrichtung getrennt und sind daher vor Remote-Angriffen geschützt.
- Um der zunehmenden Ausleitung von Daten und der Drohung einer Veröffentlichung wirksam begegnen zu können, ist ein systematisches, regelgeleitetes Monitoring des Datentransfers erforderlich. So lässt sich etwa der Abfluss ungewöhnlich hoher Datenmengen erkennen und unterbinden.
- Updates der Betriebssysteme sowie der Server- und Anwendungssoftware sollten regelmäßig und zeitnah durchgeführt werden. Zur Minimierung der Angriffsfläche sollte außerdem die Anzahl der von außen zugänglichen Systeme geringgehalten und deren Nutzung durch Unbefugte erschwert werden (zum Beispiel mittels Mehrfaktor-Authentisierung, Einsatz eines Virtuellen Privaten Netzes (VPN), strengen Passwortvorgaben). Sachgerechte interne Segmentierung der IT-Netze und restriktive Administrationsrechte helfen, das Ausmaß der Schäden bei erfolgreichen Angriffen zu begrenzen.
  Für alle Institutionen sollten die umfassende und kontinuierliche Schulung aller Mitarbeiterinnen und Mitarbeiter zum Thema Informationssicherheit (Erhöhung der Aufmerksamkeit) und eine Beschränkung des administrativen Zugangs zu den Systemen auf möglichst wenige Personen selbstverständlich sein. Diese und ähnliche Maßnahmen dienen dazu, IT-gestützte geschäftskritische Prozesse möglichst resilient zu gestalten und dadurch widerstandsfähiger gegenüber Cyber-Angriffen zu machen.
- Den Auswirkungen eines kurzfristigen Ausfalls von IT-gestützten Prozessen kann zudem mit der Etablierung von alternativen oder auch redundanten digitalen Diensten begegnet werden (zum Beispiel Content Delivery Networks (CDN) für Web-Präsenz, von einem Dienstleister bereitgestellte E-Mail-Services). Die Möglichkeit zur zeitnahen Wiederherstellung solcher Prozesse dient dazu, den gegebenenfalls aus einem Ausfall resultierenden Schaden so gering wie möglich zu halten.

- Entscheidend ist hierbei, Maßnahmen für den Fall zu berücksichtigen, dass ein IT-gestützter Prozess beispielsweise durch Ransomware längerfristig nicht regulär wiederhergestellt werden kann.
- Um im Fall eines Angriffs vorbereitet zu sein, müssen Reaktionsszenarien schriftlich dokumentiert werden, die alle beschriebenen Aspekte eines Angriffs, zum Beispiel Schäden an Produktionsanlagen, den Einsatz von Personal und Sicherheitsfirmen, alternative Geschäftsprozesse oder den Reputationsverlust, als Teil des Notfallmanagements mit einbeziehen.
- Das BSI rät grundsätzlich davon ab, einer Lösegeldforderung nachzukommen, zumal in der Regel keine Garantie besteht, dass die Angreifer den Schlüssel tatsächlich herausgeben.

Köln, November 2022