CONTINUM

LÖSEGELD IST KEINE OPTION

Foto: ZVG

Gegen Cyberangriffe hilft nur die kontinuierliche Optimierung der Sicherheitsmaßnahmen. Wenn ein Unternehmen Opfer einer Attacke geworden ist, gilt es, einen kühlen Kopf zu bewahren und überlegt zu handeln. Lösegeld sollte keinesfalls gezahlt werden, das erhöht das Risko von Folgeangriffen drastisch.

Im Jahr 2022 war die Bedrohung durch Cyberangriffe laut Aussagen des BSI so hoch wie nie. Hauptbedrohung bleiben wie im Vorjahr sogenannte Ransomware-Attacken. Ransomware ist eine Art von Schadsoftware (Malware), die darauf abzielt, Benutzerdaten oder Systeme zu verschlüsseln, zu blockieren oder mit einer Veröffentlichung der Daten zu drohen, um dann Lösegeld von den Opfern zu erpressen. Ransomware-Angriffe können auf verschiedene Weise erfolgen, einschließlich Phishing-E-Mails, gefälschten Websites, Drive-by-Downloads, Exploit-Kits und Malvertising. Es ist wichtig, das Sicherheitsbewusstsein zu fördern, um Benutzer zu sensibilisieren und Best Practices für IT-Sicherheit zu implementieren. Doch was sind gute Beispiele, die den Schutz vor Ransomware möglichst hoch halten?

Immutable Backups: Die Erstellung von unveränderlichen Backups, bei denen gesicherte Daten in einem schreibgeschütz-

ten Zustand gespeichert werden, um zu verhindern, dass sie nachträglich verändert oder gelöscht werden können, ist ein probates Mittel und kann helfen, Ransomware-Angriffe zu blockieren, da die verschlüsselnden Aktivitäten der Ransomware nicht auf die Backups angewendet werden können.

Backup-Überprüfung: Funktionen zur Überprüfung von Backups untersuchen die Integrität der gesicherten Daten, um sicherzustellen, dass sie nicht durch Ransomware oder andere Bedrohungen beschädigt wurden. Diese Überprüfung kann helfen, Ransomware-Angriffe frühzeitig zu erkennen.
Regelmäßiges Patchen: Um Sicherheitslücken zu schließen und Probleme zu beheben, die die Stabilität und Funktionalität des Systems beeinträchtigen können, ist es extrem wichtig, Sicherheitsupdates beim Hardware-BIOS, beim Betriebssystem und bei der Applikation regelmäßig durchzuführen. Das gilt selbstverständlich auch für Antimalware-Software und Firewalls.

Antimalware-Software: Antivirenprogramme, Antispyware-Tools und Antimalware-Suiten sind darauf ausgelegt, Schadsoftware wie Viren, Malware, Trojaner und Spyware zu erkennen, zu blockieren oder zu entfernen. Der Echtzeitschutz der Antimalware-Software sollte aktiviert sein, um Bedrohungen schon beim Versuch aufzuspüren.

Restriktive Firewallregeln: Die Firewall-Regeln sollten restriktiv eingerichtet sein, um nur die erforderlichen Ports und Dienste für die erforderlichen Systeme zu öffnen und den Rest zu blockieren.

Segmentierung von Netzwerken: Das Unterteilen eines Netzwerks in mehrere kleinere Subnetze oder Segmente erhöht die Sicherheit und schränkt den Zugriff auf andere Segmente oder Netzwerkbereiche ein. Dadurch wird die Angriffsfläche reduziert und die Ausbreitung von Malware und Angreifern erschwert. Durch die Segmentierung können ferner spezifische Sicherheitsrichtlinien und Zugriffsregeln für jedes Segment definiert werden und Sicherheitsmaßnahmen wie Firewalls, Intrusion Detection/Prevention Systeme (IDS/IPS) und andere Vorrichtungen effektiv eingesetzt werden, um den Datenverkehr und die Kommunikation innerhalb und zwischen den Segmenten zu überwachen und zu schützen. Die Segmentierung ermöglicht auch eine Isolierung sensibler Daten und Ressourcen. Dank dieser Isolierung lässt sich der Zugriff auf diese Daten auf autorisierte Benutzer und Systeme beschränken und das Risiko unbefugter Zugriffe oder Datenlecks reduzieren.
Die Konsequenzen eines Cyberangriffs können existenzbedrohend sein. Denn Datenlecks, Ransomware-Angriffe, Phishing-Angriffe, Denial-of-Service (DoS)-Angriffe richten neben einem erheblichen finanziellen Schaden – einschließlich Kosten für Datenwiederherstellung, Haftungsansprüche von betroffenen Kunden oder Partnern und Rechtsstreitigkeiten – einen enormen Reputationsverlust an und sorgen für längere Betriebsunterbrechungen.
Außer technischen und organisatorischen Maßnahmen gelten Cyberversicherungen daher als Baustein, um die finanziellen Folgen eines Cyberangriffes und einer Datenschutzverletzung zu reduzieren und den Fortbestand des Unternehmens zu sichern. Für eine solche Versicherung zu bezahlbaren Prämien fordern die Versicherungen allerdings häufig einen Nachweis über technische und organisatorische Maßnahmen gegen Cyberangriffe. Eine angemessene Vorbereitung ist also unerlässlich, um das Risiko von Cyberangriffen zu minimieren und abzusichern.

Julian Sayer ist Vorstand für Vertrieb, Marketing und Entwicklung der Continum AG. Das Freiburger Hostingunternehmen ist AWS-, Microsoft Azure sowie IONOS Partner und unterstützt Unternehmen auf dem sicheren Weg in die Cloud.

Birkenmeier
stein+design®

Industriestraße 1 · 79206 Breisach-Niederrimsingen
Tel. 0 76 68 / 71 09-0 · www.birkenmeier.de