Gut vorbereitet für den Cyber-Ernstfall: Sophos stellt 10-Punkte-Plan für den Krisenfall bereit

Ein Incident-Response-Plan kann Unternehmen helfen, bei einer Cyberattacke die Kontrolle über die Situation zu bewahren. Sophos Labs sowie die Sophos Managed-Response- und Rapid-Response-Teams haben hierfür einen Ratgeber mit zehn entscheidenden Schritten entwickelt.

Eine Cyberattacke ist heute wahrscheinlicher als je zuvor. Studien von Sophos, wie etwa „The State of Ransomware 2021“ belegen, dass international 37 Prozent der befragten Unternehmen allein von Ransomware betroffen sind. Zwar richtete Ransomware innerhalb der letzten Jahre die vermutlich verheerendsten Schäden an, sie ist allerdings bei Weitem nicht die einzige Malware-Art, die zu ernsthaften Problemen für Unternehmen führen kann.
Organisationen und IT-Teams sind also gut beraten, sich sowohl mit wirkungsvoller Security als auch mit einer durchdachten und geprobten Incident-Response-Strategie auszustatten. Ein solcher Plan kann nicht nur Folgekosten eines Cyberangriffs minimieren, sondern viele weitere Probleme und sogar Betriebsunterbrechungen im Keim ersticken. Die Sophos Labs haben ihre Erfahrungen zusammen mit dem Sophos-Managed-Response und Sophos-Rapid-Response-Team gesammelt und stellen das Ergebnis im „Incident Response Guide“ zur Verfügung.:

1. **Alle Beteiligten und Betroffenen festlegen**
   Nicht allein das Sicherheits-Team ist verantwortlich und von Angriffen betroffen, sondern viele weitere Personen im Unternehmen. Vom C-Level über Abteilungsleitungen bis hin zur Rechts- oder HR-Abteilung gilt es, die entscheidenden Personen zu identifizieren und in die Incident-Planung aktiv einzubeziehen. Zu diesem Zeitpunkt sollten zudem alternative Kommunikationsmöglichkeiten in Betracht gezogen werden, da ein Ausfall der IT auch die klassischen Kommunikationskanäle betreffen kann.
2. **Kritische Ressourcen identifizieren**
   Um eine Schutzstrategie zu erarbeiten und im Ernstfall das Ausmaß und die Folgen eines Angriffs bestimmen zu können, müssen die Ressourcen, die für das Unternehmen die höchste Priorität haben, ermittelt werden. Nur so können im Ernstfall die unternehmenskritischsten Systeme gezielt und mit hoher Priorität wiederhergestellt werden.
3. **Ernstfall-Szenarien üben und durchspielen**
   Übungen sorgen dafür, dass bei einem Cyberangriff koordiniert, schnell und zielgerichtet gehandelt werden kann. Ein Plan ist dann besonders gut, wenn alle Beteiligten jederzeit genau wissen, was sie umgehend zu tun haben, anstatt erst nach einer Handlungsanleitung zu suchen oder gar zu versuchen, intuitiv zu handeln. In den Übungen sollten zudem unterschiedliche Angriffsszenarien definiert sein.
4. **Security-Tools bereitstellen**
   Ein sehr wichtiger Teil des Schutzes und damit auch des Incident-Response-Plans sind präventive Maßnahmen. Dazu gehören auch geeignete Security-Lösungen für Endpoints, das Netzwerk, die Server und die Cloud sowie für Mobilgeräte und E-Mails. Wichtig bei den Tools sind ein hoher Grad an Automation, etwa durch den Einsatz von KI, sowie eine transparente und integrierte Verwaltungs- und Alarmkonsole, um potenzielle Angriffe zum frühestmöglichen Zeitpunkt zu erkennen und im Idealfall automatisch zu eliminieren.
5. **Maximale Transparenz sicherstellen**
   Ohne die erforderliche Transparenz über alle Vorgänge während eines Angriffs haben Unternehmen Schwierigkeiten, angemessen zu reagieren. IT- und Sicherheitsteams sollten über das nötige Handwerkszeug verfügen, um das Ausmaß und die Folgen eines

Angriffs zu bestimmen – einschließlich der Ermittlung von Eintrittspunkten und Persistenzpunkten der Angreifer.

6. **Zugriffskontrolle implementieren**
   Angreifer nutzen schwache Zugriffskontrollen aus, um die Abwehr zu unterwandern und um ihre Berechtigungen auszuweiten. Wirksame Zugriffskontrollen sind daher unerlässlich. Hierzu gehören unter anderem die Bereitstellung einer mehrstufigen Authentifizierung, die Beschränkung von Administrator-Rechten auf möglichst wenige Konten. Für manche Unternehmen kann es sinnvoll sein, ein zusätzliches Zero-Trust-Konzept zu erstellen und mit den geeigneten Lösungen und Services zu realisieren.
7. **In Analyse-Tools nutzen**
   Neben der Sicherstellung der erforderlichen Transparenz sind Tools, die während einer Untersuchung den erforderlichen Kontext liefern, enorm wichtig. Dazu zählen Incident Response Tools wie EDR (Endpoint Detection and Response) oder XDR (Extended Detection and Response), mit denen die gesamte Umgebung nach Indicators of Compromise (IOCs) und Indicators of Attack (IOA) durchsucht werden kann.
8. **Reaktionsmaßnahmen festlegen**
   Eine Attacke rechtzeitig zu erkennen ist gut, jedoch nur die halbe Miete. Denn nach der Entdeckung geht es darum, den Angriff einzugrenzen beziehungsweise zu eliminieren. IT- und Sicherheitsteams müssen in der Lage sein, eine Vielzahl von Reaktionsmaßnahmen zum Stoppen und Beseitigen von Angreifern einzuleiten – je nach Angriffsart und Schwere des potenziellen Schadens.
9. **Awareness-Trainings durchführen**
   Alle Mitarbeiter eines Unternehmens sollten sich der Risiken bewusst sein, die sie unter Umständen mit ihren Handlungen auslösen. Daher ist ein Training ein wichtiger Teil eines Incident-Response-Plans beziehungsweise der Prävention. Mit Tools zur Angriffssimulation lassen sich reale Phishing-Angriffe auf Mitarbeiter ohne Sicherheitsrisiko simulieren. Je nach Ergebnis helfen spezielle Trainings die Mitarbeiter zusätzlich zu sensibilisieren.
10. **Managed Security Services**
    Nicht jedes Unternehmen hat die Ressourcen, einen Incident-Response-Plan und vor allem ein Incident-Response-Team mit ausgewiesenen Experten intern zu realisieren. Abhilfe schaffen Dienstleister wie MDR-Provider (Managed Detection and Response). Sie bieten 24/7 Threat Hunting, Analysen und Reaktion auf Vorfälle als Managed Service. MDR- Services helfen Unternehmen nicht nur auf Vorfälle zu reagieren, sie senken gleichzeitig die Wahrscheinlichkeit eines Vorfalls

„Bei einem Cybersecurity-Vorfall zählt jede Sekunde und für die meisten Unternehmen ist es nicht die Frage, ob sie betroffen werden, sondern lediglich wann der Angriff geschieht“, erklärt Michael Veit, Security-Experte bei Sophos. „Dieses Wissen ist nicht neu. Unternehmen unterscheiden sich vor allem dadurch, ob sie dieses Wissen mit entsprechenden Vorkehrungen umsetzen oder ob sie das Risiko eingehen, ihre Existenz aufs Spiel zu setzen. Es ist ein bisschen wie mit dem Anschnallen im Auto – ohne Sicherheitsgurt bei einem Unfall unversehrt zu bleiben ist sehr unwahrscheinlich. Ein gut vorbereiteter und durchdachter Incident-Response-Plan, den alle betroffenen Parteien im Unternehmen sofort umsetzen können, kann die Folgen eines Cyberangriffs erheblich abmildern.“

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de