RheinlandPfalz
LANDESKRIMINALAMT

ORIENTIERUNGSHILFE „CYBERANGRIFF“

Mainz, 07.09.2018

Mit der Orientierungshilfe „Cyberangriffe“ möchte das Landeskriminalamt Rheinland-Pfalz Wirtschaftsunternehmen und anderen öffentlichen und nicht-öffentlichen Institutionen eine Orientierungshilfe im Zusammenhang mit Cyberangriffen zur Verfügung stellen. Sie soll die Handlungssicherheit in diesen Fällen verbessern, ohne dabei bindenden Charakter zu entfalten.

Die Realisierbarkeit der einzelnen, nicht abschließend aufgeführten, Maßnahmen sowie deren Kombination bedürfen jeweils einer konkreten Einzelfallbetrachtung im Hinblick auf die vorhandene Unternehmensstruktur sowie auf das jeweilige Geschäftsmodell.

Präventivmaßnahmen:

- Kenntnisnahme möglicher Bedrohungsszenarien
- Umsetzung des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als Grundlage eines professionellen Sicherheitskonzeptes
- Regelmäßige Identifizierung des Schutzbedarfs von Daten und Systemen
- Nutzung eines vielschichtigen Verteidigungssystems (bspw. bestehend aus Firewalls, Intrusion Detection Systemen, E-Mail-Filterregeln sowie Antivirenprogrammen) zur Verhinderung der Verbreitung der Schadsoftware
- Regelmäßige Durchführung von Updates für die eingesetzten Softwareprodukte und Betriebssysteme
- Deinstallation nicht mehr benötigter oder unsicherer Software
- Nutzung einer Server- und Desktop-Virtualisierung (sofern möglich) um die betroffenen Systeme schnell neu auf- oder zurücksetzen zu können
- Speicherung besonders sensible Geschäftsdaten in einem isolierten Netzwerk

- Regelmäßige Beobachtung der internen Netzwerke und Kontrolle der Gateways zwischen den Netzwerksegmenten
- Physikalische Trennung von Netzwerksegmenten (sofern möglich)
- Einstellung der E-Mail-Server in der Form, dass die Annahme externer Mails mit internem Absender verhindert wird
- Überprüfung aller E-Mails auf die richtige Absenderadresse sowie die korrekte Schreibweise der E-Mail Domain
- Besondere Achtsamkeit bei Eingang von E-Mails von unbekannten Absendern mit Anhängen oder LINKS (es könnte sich um Schadcode handeln)
- Deaktivierung der Ausführung von Skripten (sofern möglich) sowie Abschaltung nicht benötigter Protokolle (bspw. SMB1)
- Verwendung von Verschlüsselungsmechanismen (z.B. Verschlüsselung von Datenträgern) und digitale Signatur der E-Mails im Rahmen der internen und externen E-Mail-Kommunikation[1]
- Regelmäßig Durchführung von Backups auf getrennten Systemen/Netzwerken zur Datensicherung und Überprüfung der Wiederherstellbarkeit der Daten
- Ablage wichtiger Daten auf Netzlaufwerken, da lokale Dateien unter Umständen nicht vom Backup erfasst werden
- Aufbewahrung der jeweils durchgeführten Backups über einen längeren Zeitraum bevor diese wieder überschrieben werden
- Einschränkung der Zugriffsberechtigungen auf das Nötigste; Über Administratorenrechte sollten nur ganz wenige ausgewählte Personen verfügen. Vergabe, sofern möglich, von ausschließlichen Leserechten für einzelne Benutzer. Auch ein restriktiver Umgang mit Leserechten kann zum Schutz Ihrer Daten beitragen
- Durchführung von Zugriffsprotokollierungen / Regelmäßige Sichtung der Logs
- Verwendung sicherer (starker) Passwörter und regelmäßige Änderung dieser. Eine höhere Sicherheit bieten bspw. Zwei-Faktor-Authentifizierungen[2]

[1] BSI: Wie verschlüsselt kommunizieren?
www.bsi-fuer-buerger.de [...] Verschluesselung

[2] BSI: Zwei-Faktor-Authentisierung bezeichnet die Kombination von zwei Authentisierungstechniken, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte.
https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/glossar_node.html

- Durchführung von Awareness-Kampagnen (z.B. Sensibilisierung und Schulung der Mitarbeiter/-innen)
- Definition der Anforderungen an Geschäftspartner oder Dienstleister
- Erstellung von IT-Sicherheitskonzepten, Sicherheitsrichtlinien und Notfallplänen
- Durchführung eines firmeninternen Controllings
- Austausch mit anderen Unternehmen und Behörden zu aktuellen Bedrohungen
- Vorbereitung Presse- und Öffentlichkeitsarbeit (interne Abstimmung / Meldewege für die etwaige Erstellung einer Erstmeldung

Erreichbarkeiten:

- Erstellung und Vorhalt von Listen mit den Erreichbarkeiten der Entscheidungsträger / Ansprechpartner (möglichst in Papierform – Hinterlegung nur bei den Entscheidungsträgern!)
    - Geschäftsführer, Vorstand, Inhaber, ggf. Prokurist (vertretungsberechtigt)
    - Chief Information Officer (CIO) bzw. Chief Information Security Officer (CISO)
    - (System-) Administrator
    - Datenschutzbeauftragter
    - Leiter Rechtsabteilung
    - Betriebsrat / Arbeitnehmervertretung
    - Presse- und Öffentlichkeitstelle des Unternehmens
- Sofern externe IT-Dienstleister eingebunden sind, sollten deren Erreichbarkeiten analog vorgehalten werden und bereits im Vorfeld deren Kooperation sowie ein direkter Informationsaustausch im Schadensfall sichergestellt sein
- Erreichbarkeit der Zentralen Ansprechstelle Cybercrime für rheinland-pfälzische Wirtschaftsunternehmen, öffentliche und nichtöffentliche Stellen (ZAC) hinterlegen.
    - **ZAC –Hotline: 06131/65-2565**
    - **E-Mail-Adresse der ZAC: lka.cybercrime@polizei.rlp.de**

Vorhalt einer fortlaufend aktualisierten IT-Laufkarte mit Informationen zu:

- Netzplan/Netzstruktur
- Angaben zur Serverstruktur (Standort/Vernetzung)
- Erreichbarkeiten (s.o.)
- Passwörtern
- Festlegung und Bereitstellung von Ersatzservern (für den Notfall)
- Internetanschlüssen innerhalb des Unternehmens
- Weiteren Netzwerkzugänge innerhalb des Unternehmens
- Kenntnis der Zugangsdaten (sofern Cloud-Dienste genutzt werden)

Ermittlungsunterstützende Maßnahmen:

- Erstellung einer identischen Kopie des betroffenen Systems - wenn möglich mit Hauptspeicherdump - für eine spätere Analyse und als Nachweis für das durch den Angriff geschädigte System (Auflistung der Schäden und Kosten)
- Falls System nicht vom Internet getrennt werden kann, Protokollierung des Netzverkehrs (mit z.B. WireShark)
- Sicherung aller relevanten, bereits bestehenden Protokolle bzw. Logdateien
- Zeitpunkte, d.h. Daten und Uhrzeiten (einschließlich Zeitzone), an dem relevante Ereignisse entdeckt wurden bzw. stattfanden
- Angaben (Namen, Daten, Uhrzeiten) zu relevanten Telefonanrufen, E-Mails und anderen Verbindungen
- Identitäten der Personen, die im Zusammenhang mit dem Schadensfall Aufgaben bearbeiten, eine Beschreibung dieser Aufgaben und der Zeitaufwand
- Systemadministrator muss zur Herausgabe von Informationen an die Polizei berechtigt sein
- Benennung der von dem Angriff betroffenen Serversysteme (Netze), Software, Datenbanken sowie die Art der Beeinträchtigung.
- Sind die Systeme durch Passwörter geschützt?
- Angaben zu Umfang und Art der IT-Sicherheit (Firewall, Viruswall, Intrusion Detection System, Virenschutz etc.)
- Angaben zu Umfang und Art des entstandenen Schadens

Wichtige Hinweise

- Aktuelle Maßnahmen sollten keine Veränderungen am Systembetrieb oder den gespeicherten Dateien herbeiführen!
- Keine eigenen offensiven Gegenmaßnahmen, da die Angriffe häufig von kompromittierten Systemen Dritter (möglicherweise unbeteiligter Personen) ausgehen.
- Die zuständigen Personen in Ihrer Firma sollten unverzüglich über den Angriff und alle Ergebnisse der bisherigen Analyse informiert werden (über geschützte Kommunikationskanäle).
- Die Polizei wird die erhaltenen Hinweise vertraulich behandeln!

Herausgeber
Landeskriminalamt Rheinland-Pfalz
Abteilung 4 / Dezernat 47 - Cybercrime
Valenciaplatz 1-7
55118 Mainz
E-Mail: lka.cybercrime@polizei.rlp.de
Internet: www.polizei.rlp.de