Baden-Württemberg

LANDESKRIMINALAMT

Warnmeldung für Wirtschaftsunternehmen im Handel

Unberechtigte Netzwerkzugriffe in Zusammenhang mit E-Mail-SPAM

Stuttgart, 16.12.2024

Der beim Landeskriminalamt Baden-Württemberg eingerichteten Zentralen Ansprechstelle Cybercrime (ZAC) ist eine Häufung von Angriffen mit dem Ziel der Erlangung von unerlaubten Netzwerkzugriffen auf die IT-Infrastruktur von Wirtschaftsunternehmen bekannt geworden. Bitte sensibilisieren Sie die zuständigen Mitarbeiterinnen und Mitarbeiter Ihres Unternehmens und informieren Sie diese über das Vorgehen der Täter und über die Handlungsempfehlungen.

Wie gehen die Angreifer vor?

Die Tathandlung beinhaltet drei Schritte:

1. Zunächst überfluten die Angreifer ausgewählte, geschäftliche E-Mail-Postfächer des betroffenen Unternehmens mit einer massiven Welle an SPAM-E-Mails. Hierzu werden durch die Angreifer unter anderem mehrere hunderte bis tausend Newsletter-Abonnements auf die betroffenen E-Mail-Postfächer abgeschlossen. Diese sogenannte E-Mail-Bombe führt dazu, dass die Benutzer der Postfächer stark in ihrer Arbeitsfähigkeit eingeschränkt werden.

2. Im Anschluss, meist nach mehreren Stunden oder Tagen, meldet sich der Angreifer direkt bei den Benutzern der betroffenen E-Mail-Postfächer. Der Angreifer verwendet hierzu in der Regel eine durch das betroffene

Unternehmen genutzte Kommunikations- oder Chat-Plattform. Der Angreifer gibt vor, mit der Beseitigung des Problems beauftragt worden zu sein und verleitet den betroffenen Benutzer dazu, ihm über die genutzte Kommunikations- oder Chatplattform Zugriff auf den Rechner zu gewähren.

3. Sobald die Steuerung des Rechners durch den betroffenen Benutzer freigegeben wurde, versucht der Angreifer, fremde Programme und/oder Schadsoftware auf den betroffenen Rechner nachzuladen und zu installieren. Insbesondere die Installation von Fernzugriff- und Wartungs-Softwarelösungen konnte festgestellt werden. Ziel des Angreifers ist hier die Schaffung eines dauerhaften Zugangs zur IT-Infrastruktur des betroffenen Unternehmens.

Nach Schaffung des Zugangs konnte beobachtet werden, dass durch den Angreifer versucht wird, Unternehmensdaten auszuspähen, zu exfiltrieren sowie weitergehende Nutzerfreigaben einzurichten oder zu verändern. In einem Fall kam es wenige Tage nach dem Vorfall unter Verwendung eines Verschlüssungstrojaners zu einem sogenannten Ransomware-Angriff auf IT-Infrastruktur des betroffenen Unternehmens.

Handlungsempfehlungen

Für IT-Verantwortliche:

- Prüfen Sie, ob die Steuerungsfunktionalität der Kommunikations- und Chatplattform global aktiviert ist. Deaktivieren Sie diese, sofern nicht unternehmensrelevant.
- Unterbinden Sie die Möglichkeit von externen RDP-Verbindungen durch entsprechende Konfiguration der Firewall. Implementieren Sie für RDP-Verbindungen eine Allowlist.
- Passen Sie die entsprechenden Gruppenrichtlinen an, um die Installation von externer RDP-Software zu verhindern.
- Stellen Sie sicher, dass Sie auch offline (telefonisch) von Mitarbeitern erreicht werden können.
- Überprüfen Sie die Einstellungen Ihrer Mail-Server, insbesondere der des SPAM-Filters, bei einer vorliegenden SPAM-Welle.

Für Mitarbeiter:

- Kontaktieren Sie proaktiv den oder die firmeninternen IT-Verantwortlichen, falls Ihr Postfach von SPAM-E-Mails überflutet wird.
- Seien Sie generell misstrauisch, falls sich eine unbekannte Person meldet und Ihnen bei IT-Problemen helfen möchte. Fragen Sie nach einer Rückrufmöglichkeit, gleichen diese ab und lassen Sie sich den Auftrag von Ihrer IT oder Ihrem Vorgesetzten bestätigen.
- Sollten Sie einer fremden Person dennoch Zugriff gewährt haben, trennen Sie Ihren Rechner sofort vom Netzwerk, indem Sie das Netzwerkkabel ausstecken und informieren Sie unverzüglich den IT-Verantwortlichen Ihres Unternehmens. Schalten Sie den betroffenen Rechner nicht aus.

Ihre Organisation ist Opfer des oben beschriebenen IT-Sicherheitsvorfalles geworden?

- Ergreifen Sie umgehend Maßnahmen zum Schutz Ihrer IT-Infrastruktur: Trennen Sie Ihre Backups, Veranlassen Sie die Quarantäne des betroffenen Rechners, Prüfen Sie bestehende Netzwerkverbindungen.
- Erstatten Sie unverzüglich Anzeige bei der Polizei.
- Für Unternehmen und Behörden mit Sitz in Baden-Württemberg ist zudem die beim Landeskriminalamt eingerichtete Zentrale Ansprechstelle Cybercrime (ZAC) Ansprechpartner in allen Belangen des Themenfeldes Cybercrime erreichbar.
- Kontaktdaten der ZAC: Telefon: +49 (0)711 5401-2444,
  E-Mail: cybercrime@polizei.bwl.de, Website: www.lka-bw.de/zac
- Die Kontaktdaten der ZAC-Dienststellen anderer Bundesländer können Sie auf der folgenden Webseite nachlesen: www.polizei.de/zac