TAGESSPIEGEL
BACKGROUND

Cybersecurity

Cyberangriffe: Zwei Unternehmen berichten

Aus Angst vor Reputationsschäden oder öffentlicher Kritik schweigen viele Unternehmen nach einem Cyberangriff. Dabei kann der Austausch anderen Unternehmen dabei helfen, im Ernstfall handlungsfähig zu bleiben. Zwei betroffene Unternehmen berichten von ihren Erfahrungen, ihren Gegenmaßnahmen und geben Tipps.

von **Ulrich Hottelet**

veröffentlicht am 13.12.2022

Wer mit Unternehmen sprechen möchte, die von einem Cyberangriff betroffen waren, sammelt meist Absagen ein. Zu groß ist die **Angst vor einem Reputationsschaden**. Doch in den vergangenen Jahren hat sich die Einstellung gewandelt. Klar ist mittlerweile, dass es keinen hundertprozentigen Schutz gegen das Eindringen von Cyberkriminellen gibt.

Entscheidend ist vielmehr, dass die Attacke so schnell wie möglich entdeckt und ihr Ausbreiten so effektiv wie möglich beschränkt wird, damit der wirtschaftliche Schaden minimiert wird. Inzwischen wissen das auch viele Unternehmen. Sie sind daher bereitwilliger geworden, über ihre Erfahrungen mit Angriffen und ihren Gegenmaßnahmen zu sprechen. Einige von ihnen haben auch das größere Ganze im Auge, denn der Austausch und das Teilen von Lehren, kommt am Ende auch dem **Wirtschaftsstandort Deutschland** zugute.

Ein aktueller Fall aus diesem Jahr ist das **Abfallentsorgungsunternehmen Otto Dörner**. Es begann damit, dass Mitte Januar bei einer Wartung der Systeme eine Anomalie entdeckt wurde: Immer mehr Dateien enthielten eine kryptische Endung als Dateityp. Die betroffenen Systeme – der größte Teil davon im Rechenzentrum – wurden isoliert und heruntergefahren. Datenbanken und Anwendungsdateien liefen nicht mehr.

Lösegeld zahlen – ja oder nein?

„Dafür fanden wir eine Textdatei der Täter mit dem Titel „How to decrypt“ mit Onion-Adressen und einer typischen Ransomware-Nachricht“, berichtet IT-Leiter **Stefan Stelling**. Der Angriff zielte auch auf die Büro-Infrastruktur, wurde aber von deren Endgerät-Virenschutz erfolgreich abgewehrt. Daher hat Dörner inzwischen den Büroschutz auch im Rechenzentrum installiert. Mittels **Forensik** fand man heraus, dass der Angriff über ein kompromittiertes Nutzerkonto eines Dienstleisters erfolgt war, der über keine Zwei-Faktor-Authentifizierung verfügte.

Ein Tag vor der Verschlüsselung waren die Zugangsdaten wahrscheinlich im Dark Web gehandelt worden. Indizien dafür waren eine Probe-Transaktion und **Zugriffe von einem russischen Provider** aus, die durch forensische Untersuchung erkannt wurden. „Die Täter wollten eine siebenstellige Summe per Bitcoin erpressen“, sagt Stelling. „Wir haben uns gleich an die Cyberkriminalitätsabteilung des LKA gewandt und dann zusammen die Onion-Adresse aufgerufen, die speziell für Dörner eingerichtet worden war.“ Bemerkenswert ist der Sarkasmus der Täter: Die Ansprechpartner für das Unternehmen nannten sich **Sales Department**. Landeskriminalamt (**LKA**) und Dörner waren sich einig, dass eine Lösegeldzahlung nicht in Frage kommt.

Da eine Entschlüsselung zu lange gedauert hätte, nachdem alles einzeln verschlüsselt worden war, kam es darauf an, **Zeit zu gewinnen**. „Ich habe mich in der Kommunikation mit den Tätern dumm gestellt, um sie hinzuhalten. Zum Beispiel tat ich so, als wüsste ich nicht, wie man Bitcoin überweist.“ Zwei Monate lang zog sich der Austausch mit den Angreifern

hin, eine Zeitspanne, während der alle paar Tage Nachrichten geschrieben wurden. Die Kriminellen drohten mit der **Veröffentlichung von Daten**. Schließlich ließen sich die Angreifer nicht länger hinhalten und starteten eine massive DDoS-Attacke auf Dörners Website.

Mit Notfallplänen durch die Krise

Da die meisten Windows-Systeme verschlüsselt worden waren, entschied sich das Unternehmen nach Beratung mit einem **Incident-Response-Dienstleister**, seine IT-Landschaft neu aufzubauen und so künftig für mehr Sicherheit zu sorgen. „Wir wollten das ohnehin machen und haben schon am ersten Tag des Angriffs damit losgelegt. Es dauerte aber bis Mitte 2022 bis zur Fertigstellung", sagt Stelling. Denn neben der neuen Sicherheitsarchitektur wurde auch ein Lifecycle-Management eingeführt, Datenflüsse und prozessuale Abläufe optimiert. Die Übergangszeit wurde mit **Notfallplänen** gemanagt.

Die 350 LKWs von Dörner konnten täglich fahren, auch wenn die Planung teilweise händisch statt digital gemacht werden musste und die Telekommunikation einige Tage lang nicht funktionierte. „Unser Geschäftsmodell erwies sich als resilient gegen IT-Angriffe, zum Beispiel weil es einen zweiten Ablageort für die Tourenplanung gab", so Stelling. Großteils konnte der **Geschäftsbetrieb** also weiterlaufen. Den finanziellen Schaden kann der IT-Leiter daher nicht beziffern. Erfreulicherweise reagierten die Kunden verständnisvoll, wenn es zu Verzögerungen bei Rechnungen kam, die Mitarbeiter zeigten hohes Engagement.

Wisag wird Opfer der Hive-Gruppe

Ähnlich leidvolle Erfahrungen mit einem Ransomware-Angriff machte die **Wisag Unternehmensgruppe** (*Background berichtete (https://background.tagesspiegel.de/cybersecurity/wir-brauchen-mehr-oeffentliche-bekenntnisse-zu-cyberangriffen)*), einer der größten Multi-Dienstleister Deutschlands in Luftfahrt, Gebäudetechnik und Industrie-Services. Ebenfalls im Januar dieses Jahres bemerkten Mitarbeiter merkwürdige Effekte im System. „Plötzlich wurden lokale Firewalls aktiv.

Nach einer halben Stunde stellten wir mit einem Dienstleister fest, dass wir gehackt worden waren“, berichtet IT-Leiter **Michael Futterer**.

Auf jedem Server fand sich eine Textdatei auf Deutsch und Englisch, die dazu aufforderte, keine Polizei einzuschalten, sondern mit der „Sales-Abteilung“ unter einer angegebenen Dark-Web-Adresse Kontakt aufzunehmen. „Da fast alles verschlüsselt war, haben wir umgehend alle Systeme ausgeschaltet“, sagt Futterer.

Wisag kontaktierte die Täter nicht, sondern informierte vielmehr das LKA. Die Prüfung der Textdatei ergab, dass die **„Hive“-Gruppe** hinter der Attacke steckte. Deren Malware ist ein Erpressungstrojaner. Nach Angaben des FBI hat sie bislang 100 Millionen US-Dollar in die Kassen der Gruppe gespült. Seit Mitte 2021 hat sie weltweit über 1.300 Firmen erpresst. Wisag entschloss sich zum Schritt in die Öffentlichkeit und gab wenige Tage später eine Pressemitteilung heraus, wonach das Unternehmen die Sicherheitsbehörden eingeschaltet hat, um die Täter zu ermitteln (*Background-Interview Vorstand mit Michael C. Wisser (https://background.tagesspiegel.de/cybersecurity/wir-brauchen-mehr-oeffentliche-bekenntnisse-zu-cyberangriffen)*).

Forensische Analyse führt zu Phishing-Mail

Intern war ein Notfallplan vorhanden, dessen Meldeketten befolgt wurden. Als IT-Sicherheitsdienstleister wurden zwei vom Bundesamt für Sicherheit in der Informationstechnik (**BSI**) zertifizierte Firmen engagiert. Anschließend wurde jedes System gescannt. Die befallenen Systeme wurden **aus dem Backup per Snapshot wiederhergestellt**. Das sind virtuelle Abbilder der Blöcke auf der Festplatte. So funktionierte vier Tage nach dem Angriff das Mailsystem wieder und eine Woche später die wichtige Lohnabrechnung für über 50.000 Mitarbeiter.

„Nach einigen Tagen hätten wir theoretisch wieder normal arbeiten können, aber die forensische Analyse dauerte drei Monate“, sagt Futterer. Der Zeitraum war unter anderem deshalb so lang, weil sich die Prüfung eines Systems über **zehn Stunden** hinziehen kann. Die Systeme wurden entsprechend ihrer Priorität mit Blick auf den finanziellen Schaden nacheinander geprüft und wiederhergestellt.

Auch die **Backups** wurden forensisch überprüft. „Es war unglaublich viel zu tun: von der Wiederherstellung über Bereitstellungen bis hin zu anschließenden Tests der Operative“, berichtet der IT-Leiter. Darüber hinaus wurde gleichzeitig eine neue IT-Landschaft gebaut, in der die Forensik höchste Priorität hat. Sehr viel Zeit gekostet hat auch die nötige **„Sauberkeitsbestätigung“** durch einen BSI-zertifizierten Anbieter.

„Es entspricht unserer Haltung und unserem Leistungsversprechen an unsere Kunden, dass wir dem Thema Sicherheit grundsätzlich höchste Priorität zuordnen. Darüber hinaus gibt es einige Unternehmen unter unseren Kunden, die den Vorschriften der Kritischen Infrastruktur unterliegen, zum Beispiel Flughäfen und Banken. Diese haben eine solche Zertifizierung verlangt, auch wenn es keine gesetzliche Pflicht ist.“ Eines der forensischen Ergebnisse war, dass der Angriff wahrscheinlich mit einer **Phishing-Mail** begann, die einen Link zu einer infizierten Site enthielt. Der operative Schaden für Wisag ist nicht bezifferbar.

Was hilft in der Krise?

Als wichtigste Tipps für andere Unternehmen gibt Stelling, schon vorab für eine **stringente Notfallorganisation** zu sorgen und einen Krisenstab einzurichten. Nach einer Attacke sollte man schnell und transparent nach innen und außen kommunizieren. Generell sollte die Zwei-Faktor-Authentifizierung eingerichtet sein und die Maßgabe des Zero Trust gelten: „Immer wieder die Credentials überprüfen, Authentifizierung verlangen und den Zugang beschränken“, empfiehlt er.

Auch Futterer rät zur **Segmentierung von Accounts**, damit Angreifer weniger Zugriffsmöglichkeiten haben. Die Notfallliste des BSI sollte man in einer Schublade vorhalten und Vorkehrungen treffen wie Meldelisten aufstellen. Ein **kontinuierliches Awareness-Training** ist wichtig, um die Mitarbeiter zu sensibilisieren. Zudem betont Futterer, wie wichtig Backups sind. Sie sollten in einem komplett separaten Bereich außerhalb der Domäne mit einer **Read-only-Technologie** aufbewahrt werden.