Quelle: greenbutterfly | AdobeStock

Systemhäuser als Sprungbrett für Cyberangriffe

Der Katalysator als Zielscheibe

Unternehmen wie auch öffentliche Einrichtungen brauchen IT-Dienstleister, Software- und Systemhäuser als Katalysatoren für ihre Digitale Transformation. Gerade deshalb geraten IT-Provider ins Visier der Cyberkriminellen.

Wilhelm Greiner | Wer Mitte Juni in Frankfurt online eine Sperrmüllabholung buchen wollte, musste enttäuscht feststellen: Service nicht verfügbar. Zeitgleich waren die Webseiten der Mainzer Stadtwerke nicht zu erreichen. Der Ticketverkauf für den Mainzer Nahverkehr war teilweise gestört, ebenso der in Darmstadt. 1.800 Beschäftigte der Mainzer Stadtwerke kamen nicht an ihre E-Mails, die 2.000 Angestellten des Darmstädter Energieversorgers Entega auch nicht. Außerdem ließen sich die Homepages einiger Gemeinden im Odenwaldkreis nicht mehr aufrufen. Was war passiert?

Supply-Chain-Angriffe haben sich etabliert

Entegas IT-Tochter Count + Care versorgt eine Reihe umliegender Kommunen und kommunaler Betriebe mit IT-Dienstleistungen. Normalerweise. Doch Count + Care war einem Ransomware-Angriff zum Opfer gefallen, wie Entega am 12. Juni per Twitter bekanntgab. Nach Angaben örtlicher Zeitungen war ein Mitarbeiter des IT-Dienstleisters auf eine Phishing-Mail hereingefallen und hatte einen Anhang mit Schadsoftware geöffnet. Die Erpresser forderten laut Medienberichten (die allerdings weder die Polizei noch Entega bestätigten) 15 Millionen Euro Lösegeld. Der Darmstädter Versorger zahlte nicht und brauchte dann dreieinhalb Wochen, um seine Systeme aus Backups wiederherzustellen. Wichtig zu wissen: Laut Entega war die Versorgung mit Strom, Gas, Wasser oder TK-Dienstleistungen zu keiner Zeit vom Angriff betroffen.

Risiko Supply-Chain-Angriff

Erleidet ein Unternehmen – oder eben einen kommunalen Versorger – über den Umweg eines IT-Dienstleisters oder Softwarehauses Schaden, sprechen Fachleute von einem Supply-Chain-Angriff. Diese sind bei Weitem nicht neu:

Anfang 2020 – die Älteren werden sich erinnern – kompromittierten Angreifer die Update-Server des US-Softwareanbieters SolarWinds, sodass die Server Software mit Schadcode auslieferten – an mehrere Tausend Kunden, darunter diverse US-Behörden, bis hin zum Pentagon. Als Drahtzieher – wenn denn die hardwarelastige Formulierung bei einem Softwarehaus angebracht ist – vermuteten Experten den russischen Geheimdienst SVR.

Welle russischer Ransomware-Attacken

Im Juli 2021 fielen dann zahlreiche Managed Services Provider (MSPs) und in der Folge deren Kunden, darunter auch deutsche Unternehmen, einem Ransomware-Angriff der REvil-Gruppe zum Opfer, die – Zufälle gibt's! – ebenfalls aus Russland stammt. REvil nutzte Sicherheitslücken in der Software VSA des ebenfalls US-amerikanischen Anbieters Kaseya, um Schadsoftware zu verteilen. VSA dient dem Fernzugriff auf IT-Systeme, weshalb viele MSPs zur Klientel zählen. Der Fall schlug hohe Wellen: US-Präsident Biden beschwerte sich sogar telefonisch bei Putin und drohte, die USA würden gegen die Ransomware-Gruppe vorgehen, falls Russland nichts unternähme. Wenig später verschwanden die Server der REvil-Gruppe vom Netz. Zufälle gibt's!

Auch in Deutschland zielten Angreifer bereits auf die digitale Lieferkette: So wurde Ende 2021 Mediatixx aus Eltville am Rhein, ein Anbieter von Verwaltungssoftware für Arztpraxen, Opfer einer digitalen Erpressung. Und im April war dann die Website der Donau-Stadtwerke Dillingen-Lauingen offline, weil Ransomware die Systeme des Dillinger Systemhauses Reizner lahmgelegt hatte. Dieser Angriff ging auf das Konto der Gruppierung Lockbit 2.0, deren Heimat Fachleute in – man ahnt es – Russland vermuten. Lockbit 2.0 ist zugleich ein Beispiel dafür, warum Ransomware-Angriffe so stark eskalieren: Die Angreiferszene hat sich arbeitsteilig ausdifferenziert, sodass heute einem angriffslustigen Kriminellen selbst ohne tiefgehende Hacker-Kenntnisse Ransomware-as-a-Service (RaaS) zur Verfügung steht: Die eine Gruppe sammelt per Phishing Zugangsdaten ein, eine andere erzeugt den Schadcode und unterhält die Infrastruktur für deren Vermarktung. Den eigentlichen Angriff überlassen RaaS-Anbieter dann ihren „Affiliates" (Partnerunternehmen) und kassieren einen Anteil am Gewinn.


Quelle: HoSolutions

„Gegen gezieltes Phishing ist niemand zu 100 Prozent gefeit."

Manuel Atug, Head of Business Development, HiSolutions


Quelle: Bechtle

„Wir schätzen das Risiko als relativ hoch ein, dass auch über Dienstleister Cyberangriffe gefahren werden."

Christian Grusemann, Business Manager Security, Bechtle

Digitalstadt als Opfer

Der aktuelle Supply-Chain-Angriff traf nun Darmstadt – und damit eine Stadt, die sich gerne als „Wissenschaftsstadt" und neuerdings auch als „digitale Stadt" bezeichnet: Mit Gründung der Digitalstadt Darmstadt GmbH verfolgt man dort das Ziel, die Digitalisierung in allen möglichen Bereichen von Mobilität und Wirtschaft bis Kultur und Umwelt voranzutreiben – übrigens auch bei Sicherheit und Katastrophenschutz. Mit Count + Care fing sich keine Klitsche Ransomware ein, sondern ein IT-Dienstleister, der das ISO/IEC-27001-Security-Siegel trägt und als „SAP Partner Center of Expertise" zertifiziert ist. „So eine Attacke kann jederzeit bei jedem Unternehmen passieren, denn gegen gezieltes Phishing ist niemand zu 100 Prozent gefeit", sagt Manuel Atug, Head of Business Development bei HiSolutions. Der Experte für die Sicherheit kritischer Infrastrukturen (Kritis) rät: „Kritis-Betreiberinnen sollten ermitteln: Was ist der schlimmste Zustand, den eine Angreiferin über den Zugang des Dienstleisters herbeiführen könnte? Gegebenenfalls müssten sie sich dann mit der Dienstleisterin abstimmen und den Zugang einschränken, um sicherzustellen, dass höchstens eine kurze Störung, aber kein Ausfall der kritischen Infrastruktur eintreten kann."

IT-Dienstleister haben die Gefahr erkannt

Angesichts von Entwicklungen wie RaaS warnt Atug: „Die Ransomware-Gefahr wächst seit einigen Jahren, trotzdem stehen wir erst noch am Anfang. Denn hier geht es um organisierte Kriminalität und Hunderte Millionen Euro Gewinn pro Jahr, noch dazu steuerfrei – das sorgt für entsprechend hohe Motivation, viel Geld zu machen."

Gefahr erkannt

Die gute Nachricht: Die hiesigen IT-Dienstleister haben die Gefahr erkannt, zur Zielscheibe von Supply-Chain-Angriffen zu werden. „Wir schätzen das Risiko als relativ hoch ein, dass auch über Dienstleister mit entsprechenden Zugängen zu Kundensystemen Cyberangriffe gefahren werden", sagt zum Beispiel Christian Grusemann, Business Manager Security bei Bechtle. Bechtle schütze daher seine Systeme „in umfassender Weise basierend auf dem aktuellen Stand der Technik". Und Jörg Jattke, Sales Specialist Architecture & Consulting bei IT-Haus, erklärt: „Wir sehen seit einigen Jahren einen sehr starken Anstieg der Angriffsversuche, unabhängig vom Ukraine-Krieg." Für Angreifer seien Ziele interes-

sant, die viele Schnittstellen zu Kunden, Lieferanten et cetera aufweisen. „Dazu gehören auch wir als IT-Dienstleister“, so Jattke.

Erforderliche Maßnahmen

Somit stellt sich die Frage, welche Schritte nun geboten sind – seitens der Auftraggeber wie auch seitens der IT-Dienstleister. „Öffentliche Auftraggeber und die Privatwirtschaft werden nicht umhinkommen, etablierte, scheinbar vertrauensvolle Kommunikationsbeziehungen neu zu bewerten“, sagt Mario Emig, Head of Information Security Business Development bei Controlware. Wie Atug betont auch er, es gelte, Benutzerzugriffe und Zugriffe auf Daten verstärkt zu überprüfen. „Gerade die Einführung der sogenannten Zero-Trust-Strategie *(laufende Risikobewertung bei Ressourcenzugriffen ohne Vertrauensbonus für Beschäftigte, d. Red.)* sehen hier viele Experten als einen wichtigen Faktor“, so Emig. Es gehe also nicht nur um eine Maßnahme, sondern um eine abgestimmte Security-Strategie.

Hierbei erlebe das Schwachstellenmanagement eine „Renaissance“: „Ein funktionierendes, strategisches Vulnerability-Management beinhaltet weit mehr als nur das Scannen von PCs, Anwendungen und Infrastrukturkomponenten“, sagt er. „Essenzielle Aufgaben, beispielsweise das Scannen von Container-Images und die Überprüfung von Programmcode, gehören ebenfalls dazu.“ Der Log4j-Vorfall Ende 2021 habe Sicherheitsverantwortlichen erneut verdeutlicht, wie wichtig es ist, einen Überblick über die Komponenten der genutzten Software zu haben. „Nur so lässt sich im Bedarfsfall schnell eine potentielle Betroffenheit ermitteln“, so Emig. „Zusätzlich müssen wir uns darauf einstellen, dass Angriffe auf bekannt gewordene Sicherheitslücken immer schneller stattfinden.“ Controlware helfe mit Security-Strategie, -Produkten und Cybersecurity-Services, die Problematik in den Griff zu bekommen und zudem den Fachkräftemangel auszugleichen.

Sicherheit ist ein Prozess und erfordert strukturiertes Vorgehen

Zum Schutz vor Supply-Chain-Angriffen rät Christian Grusemann von Bechtle, der Zugriff auf Kundensysteme sollte ausschließlich per Jump-Server erfolgen, also über speziell für Fernzugriffe gehärtete und überwachte Server. Er rät zum Einsatz von „Privileged-Access-Management-Lösungen mit entsprechendem Session Monitoring, wann welcher Zugriff erfolgte, in Verbindung mit einer Passwort-Management-Lösung und einer Multi-Faktor-Authentisierung“.

„Wichtig ist, einen Gesamtüberblick über die IT Infrastruktur zu haben“, sagt Jörg Jattke von IT-Haus. Unternehmen sollten laut Jattke zusätzliche Lieferanten- und Kunden-Zugriffskontrollen etablieren und dabei das Least-Privilege-Prinzip anwenden, also nur das zulassen, was erforderlich ist. Zugleich warnt er davor, sich nur auf Technik zu verlassen: „Es sollten Cybersicherheit- und Awareness-Schulungen in regelmäßigen Abständen für alle Mitarbeiter durchgeführt werden“, ergänzt er. IT-Haus habe für mehr Sicherheit ein Security Operations Center (SOC) eingeführt, in dem Security-Analysten und Forensiker kontinuierlich die IT-Umgebung und Schnittstellen überwachen.

Die Frage der Verantwortung

Bei der Aufgabenteilung zwischen Kunde und IT-Dienstleister stellt sich immer die Frage, wer für was verantwortlich ist. Manuel Atug betont mit Blick auf kommunale Versorger, dass sich die Verantwortung für den ordnungsgemäßen Betrieb nicht delegieren lässt. „Erforderlich ist also eine Due-Diligence-Prüfung oder ein Technical Assessment, um zum Beispiel zu klären: Ist das Least-Privilege-Prinzip umgesetzt? Erfolgen Fernzugriffe ausschließlich mit Zwei-Faktor-Authentifizierung? Sind Zugänge von Dienstleisterinnen permanent aktiv oder werden sie individuell freigeschaltet? Letzteres ist mühseliger, aber eben auch sicherer“, so Atug.

„Sicherheit ist ein Prozess, erfordert also prozessuales, strukturiertes Vorgehen“, resümiert der Experte. „Organisationen, die diesen Security-Prozess bereits leben, haben eine entsprechende Organisations- und Fehlerkultur etabliert, idealerweise fördern sie zudem gezielt Security-Nachwuchs.“ Ist dies noch nicht der Fall, müsse das Umdenken zunächst beim Management stattfinden: „Dann lässt sich Security by Design technisch und organisatorisch umsetzen, und das Unternehmen steht nach ein oder zwei Jahren wirklich gut da.“

Systemhäuser und IT-Dienstleister sind somit heute gefordert, in doppelter Hinsicht als Katalysator zu fungieren: für die Digitalisierung, aber auch für den Wandel zu Security by Design. Denn die digitale Stadt ist immer auch eine angreifbare Stadt. IT-Service-Provider, die selbst noch keine Security-by-Design-Kultur pflegen, werden diese schnellstmöglich einführen müssen. Denn eine digitale Lieferkette ist immer auch eine angreifbare Lieferkette. ■


Quelle: Controlware

„Die Einführung der sogenannten Zero-Trust-Strategie sehen viele Experten als einen wichtigen Faktor.“

Mario Emig, Head of Information Security Business Development, Controlware


Quelle: IT-Haus

„Wir sehen seit einigen Jahren einen sehr starken Anstieg der Angriffsversuche.“

Jörg Jattke, Sales Specialist Architecture & Consulting, IT-Haus