Cybersecurity
Strategien zur Sicherheit der Lieferketten

Cyberangriffe auf Software-Lieferketten nehmen kontinuierlich zu. Erhöhte Sensibilisierung und Meldepflichten können dabei helfen, die Risiken zu verringern.

Die zunehmenden Cyberangriffe verdeutlichen, wie anfällig Software-Lieferketten sind. Dabei steigt nicht nur die Anzahl der Angriffe, sondern auch die Vielfalt und Komplexität der Angriffsmethoden. Um die Gefahren von Supply-Chain-Angriffen besser zu verstehen, lohnt sich ein Blick auf einige konkrete Vorfälle, die exemplarisch zeigen, wie unterschiedlich und doch verheerend solche Angriffe sein können. Ein Beispiel ist der Solarwinds-Angriff, bei dem Angreifer eine Backdoor in ein Software-Update einschleusten und so unbemerkt Zugang zu vielen IT-Systemen erhielten. Beim XZ Utils Angriff nutzte ein Angreifer das Vertrauen der Open Source Community und integrierte nach jahrelanger Tarnung schädlichen Code in ein beliebtes Linux-Tool (vgl. «Open Source Software», S. 52). Im Polyfill-Vorfall übernahm eine böswillige Entität die Domain einer JavaScript-Bibliothek, um Schadcode in Webanwendungen einzuschleusen. Beim Dependency-Confusion-Angriff wurden Schwächen von Paketmanagern ausgenutzt, um schadhafte Bibliotheken in Anwendungen zu integrieren. Solche Angriffe auf die Software-Lieferkette stellen für Behörden und Unternehmen ein besonders hohes Risiko dar. Angreifer können das schwächste Glied der Kette ins Visier nehmen, was ihre Erfolgschancen erheblich erhöht. Sobald sie die Lieferkette erfolgreich manipuliert haben, sind die Angriffe für nachfolgende Organisationen innerhalb der Kette nahezu nicht mehr erkennbar.

Transparenz durch Meldepflichten

Das Schweizer Informationssicherheitsgesetz (ISG) ist ein wichtiger Treiber für mehr Sicherheit in den Lieferketten. Die Einführung eines Information Security Management Systems, das die Absicherung der gesamten Lieferkette und das durchgängige Management von Cyberrisiken fordert, reduziert die Gefahren deutlich. Besonders entscheidend ist die gesetzliche Verpflichtung, die Cybersicherheit vertraglich auf die gesamte Lieferkette auszuweiten. Dies erschwert es Angreifern, gezielt das schwächste Glied zu attackieren, da die Lieferkette als Ganzes gestärkt wird.

Systeme und Strategien des Bundes

Der öffentliche Sektor spielt eine zentrale Rolle bei der Unterstützung der Unternehmen bei der Umsetzung von gesetzlichen Vorgaben. Behörden wie das Bundesamt für Cybersicherheit (BACS) sind dabei von grosser Bedeutung. Sie versorgen alle Akteure entlang der Lieferkette mit relevanten Informationen, damit Risiken realistisch eingeschätzt und gemanagt werden können. Dieser elementare Bereich der Cybersicherheit darf nicht allein privaten Unternehmen oder internationalen Organisationen wie der OWASP Foundation überlassen werden. Eine internationale Vernetzung ist dennoch notwendig, um spezifische Bedrohungen, welche die Schweizer Infrastruktur betreffen, besonders hervorzuheben. Der weltweite Ausfall durch Crowdstrike zeigt, dass es nicht ausreicht, nur kritische Infrastrukturen zu schützen. Die betroffene Software sollte laut den Allge-

meinen Geschäftsbedingungen (AGB) des Herstellers nicht in kritischen Infrastrukturen verwendet werden. In der Realität halten sich jedoch viele Unternehmen nicht daran. Dies verdeutlicht, dass Cyberrisiken für kritische Infrastrukturen nicht von einzelnen Unternehmen innerhalb der Lieferkette allein getragen werden können. Es liegt in der Verantwortung von Staat und Softwareherstellern, ein Geschäftsmodell zu entwickeln, das es ermöglicht, Softwarelösungen z. B. für kritische Infrastrukturen bereitzustellen, ohne dass dies wegen der Haftungsproblematik in den AGB generell ausgeschlossen wird.

Unsere Empfehlungen

1. Transparenz schaffen
Cyberrisiken und entsprechende Gegenmassnahmen müssen in der gesamten Lieferkette offengelegt und kommuniziert werden.

2. Information Security Management als Chance erkennen
Offener Austausch und transparente Diskussionen innerhalb der Organisation sind der Schlüssel zu einer erfolgreichen Cybersecurity-Strategie. Auch das bewusste Akzeptieren von Restrisiken ist legitim.

3. Awareness in der gesamten Organisation aufbauen
Da Angriffe oft auf das schwächste Glied abzielen, muss regelmässiges Schulungs- und Awareness-Training ein integraler Bestandteil des Information Security Managements sein.

Mehr Informationen

Kontaktmöglichkeiten und weitere Informationen zu Cybersecurity im öffentlichen Sektor:
bfh.ch/ipst/cyber-security

Kontakt

Prof. Dr. Sebastian Höhn
Dozent

sebastian.hoehn@bfh.ch
T +41 31 848 44 26