Wenn die Firewall nicht reicht…

Wie Manipulation die Lebensmittelsicherheit gefährdet

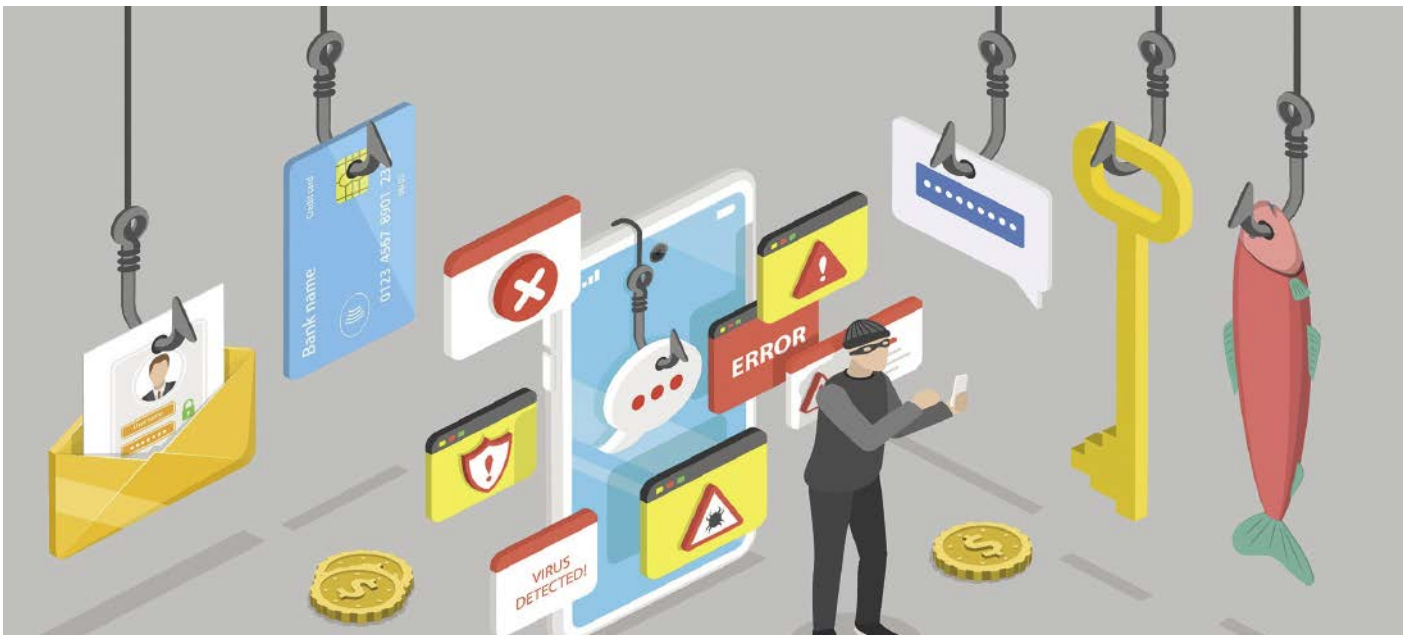

Abb.: Viele Bedrohungslagen sind branchenübergreifend vergleichbar. Doch die Lebensmittelbranche bietet spezifische Angriffsflächen bei Lebensmittelsicherheit, Hygiene und allen temperatur- und zeitkritischen Aspekten der Lieferkette.

Stefan ist ein kluger Kopf und hat ein bisschen schauspielerisches Talent. Er weiß, dass Lebensmittelbetriebe regelmäßig überprüft werden, er googelt sich den Namen eines Inspektors, bzw. auch des Produktionsleiters des Betriebes. Die Erstellung eines falschen Ausweises und der Ausdruck einer Prüf-Checkliste sind ein überschaubares Investment. Beim Besuch übt er Druck auf den Produktionsleiter aus und droht ihm mit hohen Strafen, wenn er nicht sofort die Gelegenheit bekäme, den (freilich erfundenen) Verdacht durch eine Kontrolle auszuräumen.

Mag. Julia Nusko, B. A., Calpana business consulting

Paul André de Jong, Unternehmensberatung Claudia de Jong

Stefan erhält Zutritt und nimmt sich gründlich Zeit, um Maschinen zu fotografieren, Daten zu extrahieren und anschließend die gesammelten Informationen an den Mitbewerber zu verkaufen.

Zum Glück ist Stefan nur eine Erfindung von ChatGPT. Der Modus Operandi leider nicht. Als Nahrungsmittelversorger ist die Lebensmittelindustrie ein unentbehrlicher Bestandteil der kritischen Infrastruktur Deutschlands. Komplexe Lieferketten, ein breites Spektrum an Lieferanten und die Haltung sensibler Daten machen die Lebensmittelbranche zu einem beliebten Ziel für Kriminelle.

Längst beschränken sich diese Angriffe nicht mehr auf klassische Erpressungen.

In den letzten Jahrzehnten entwickelten sich Cyberattacken zu einer zusätzlichen Bedrohung; die meisten davon finanziell motiviert, zielen sie vorwiegend auf die Störung der Verfügbarkeit der Produkte ab.

Bedrohungen durch Cyberangriffe

Cyberangriffe, die Server gezielt mit so vielen Anfragen überlasten, dass sie im schlimmsten Fall zusammenbrechen werden als Denial of Service (DoS)-Attacken bezeichnet. Bei dem speziellen Fall der gleichzeitigen DoS-Attacken als koordinierter Angriff gestartet von vielen Systemen, spricht man von Distributed Denial of Service (DDoS)-Angriffen.

Die Infiltration der Systeme mit Ransomware (meist mit der Absicht durch Verschlüsselungen der Daten hohe Geldsummen zu erpressen) oder Kompromittierung von Daten bzw. der Diebstahl derselben bedrohen (sondern auch) Deutschlands Industrie, besonders im Hinblick auf die Versorgungssicherheit und die finanzielle Stabilität.

Programmierkenntnisse sind für solche Attacken längst nicht mehr nötig; im Darknet gibt es entsprechende Tools käuflich zu erwerben („Ransomware-as-a-Service"). Als Einstiegsvektoren dienen vorwiegend verschiedene Techniken des sogenannten Social Engineerings. Im Gegensatz zu technischen Methoden, um ein System zu hacken, ist Social Engineering der nicht-technischbasierte Betrug, der Menschen dazu bringen soll, Dinge zu tun, die diese eigentlich nicht tun wollen. Das Business-Umfeld bietet dafür reichlich Gelegenheiten, um den zwischenmenschlichen Kontakt, die Hilfsbereitschaft höflicher Menschen oder das Engagement der Mitarbeiter*innen für eigene Zwecke auszunützen.

Die einfachste Form des Social Engineerings wäre etwa, drei Kaffeebecher in die Hand zu nehmen und vor der Türe zu warten. Sobald sich der erste Mensch höflich verhält, hat man sich Zutritt

zum Unternehmen verschafft, ohne auch nur ein Wort verlieren zu müssen. Schauspielerisch begabten Menschen gelingt es bisweilen telefonisch, sich als IT-Mitarbeiter*innen auszugeben und auf diese Art Angestellten ihre Passwörter zu entlocken. Buchhalter*innen zu überzeugen, man wäre ein Vorstandsmitglied („CEO-Fraud") und es müssten dringend Überweisungen durchgeführt werden, hat in manchen Unternehmen bereits Millionenschäden verursacht.

Die quantitativ beliebteste Methode für den ersten Einstieg ist jedoch der Versand getürkter E-Mails. Bekannt geworden ist dieses Vorgehen unter dem Begriff „Phishing" (eine Wortkombination aus „Password" und „Fishing", also dem Angeln nach einem Passwort). Dienten Phishing-Mails vor einigen Jahren noch durch ihre stümperhafte Bauart (schlechter Sprachgebrauch und oberflächlich kopierte Logos) unfreiwillig der Unterhaltung, so sind diese heute bereits perfekt elaboriert – auch Kriminelle entwickeln sich weiter.

Aktuell besonders beliebt und perfide ist die Integration einzelner griechischer oder kyrillischer Buchstaben, um arglose Empfänger/innen der Phishing-Mails nicht nur auf den Holzweg sondern v. a. auf den falschen Link zu führen. Hier wird mitunter der Spieltrieb, die Rätselfreude und das unpräzise Klickverhalten von Lesern für zweifelhafte Ziele missbraucht. Hand aufs Herz! Wer könnte dafür garantieren, dass falsche Buchstaben im hektischen Arbeitsalltag immer auffallen?

Viele dieser Bedrohungen („Threats") gefährden unterschiedliche Branchen in durchaus vergleichbarem Maße – wie etwa Störungen der IT-Infrastruktur, Datendiebstahl oder fehlgeleitete Finanztransaktionen bzw. Herausforderungen durch begrenzte Ressourcen für Sicherungsmaßnahmen. Allerdings hält die Lebensmittelbranche zusätzlich einige besonders vulnerable Bereiche für kriminelle Aktivitäten bereit.

Unbefugter Zutritt und HACCP

Zunächst ist der Schutz vor unbefugtem physischem Zutritt für die Lebensmittelindustrie essenziell. Unbefugtes Eindringen in heikle Produktionszonen verletzt die HACCP-Vorschriften; der Extremfall, die Produktsabotage, gefährdet unmittelbar Menschenleben.

Wie das Magazin „Focus" berichtet[1], verursachte der Rachefeldzug eines wütenden ehemaligen Mitarbeiters in einer australischen Lebensmittelkette 2018 einen kompletten Rückruf sämtlicher verkaufter Erdbeeren, da dieser Mitarbeiter Nähnadeln in selbigen platziert hatte. Insiderwissen um bauliche Strukturen und Schwachstellen in Dienstplänen, machen erzürnte (Ex-)Mitarbeiter*innen zu einer Gefahr für die Produktsicherheit.

Komplexität der Lieferketten

Eine weitere Hürde, die Lebensmittelversorger zu bewältigen haben, sind lange verzweigte Supply Chains. Auch in diesem Bereich ist die Lebensmittelbranche nicht allein mit ihren Herausforderungen, jedoch sorgt die Verderblichkeit vieler Rohstoffe für Zeitkritikalität, die Lieferketten besonders sensibel macht. Es ist erfreulich, wenn Ihr Unternehmen bestmöglich abgesichert ist, aber können Sie das auch guten Gewissens von allen mit Ihnen verbundenen Firmen behaupten? Der ENISA-Report von 2022[2] erläutert, dass Attacken über Drittfirmen 2021 für 17 % der Fälle widerrechtlichen Eindringens verantwortlich waren und deren Anteil weiter steigt. Regulatorische Anforderungen wie das NIS2-Gesetz berücksichtigen in zunehmendem Maße auch das Drittparteienrisiko.

Wie schützen wir uns?

Implementieren Sie eine klare Policy! Sie enthält Sicherheitsziele, Verantwortlichkeiten, Verfahren, Maßnahmen zur Risikominimierung, regelmäßige Reviews und die Aspekte des Drittparteienrisikos.

Sorgen Sie für regelmäßige Schulung der Mitarbeiter*innen! Diese sind entscheidend, um das Bewusstsein für Sicherheitsrisiken zu schärfen und Angestellte zu befähigen, Angriffe zu erkennen und richtig zu behandeln.

Implementieren Sie Sicherheitstechnologien! Firewalls, Intrusion Detection Systems und Verschlüsselung können dazu beitragen, die IT-Infrastruktur vor Angriffen zu schützen und den unbefugten Zugriff auf sensible Daten zu erschweren. Organisieren Sie regelmäßige Penetrationstests! Externe Dienstleister können helfen, Schwachstellen zu identifizieren und die Wirksamkeit der Sicherheitsvorkehrungen zu verbessern.

Kooperieren Sie mit Behörden und Firmen innerhalb der Branche! Nur keine falsche Scheu bei der Meldung von Sicherheitsvorfällen! Auch wenn man sich im Geschäftlichen nicht immer gerne „in die Karten schauen" lässt – der Austausch von Informationen stärkt à la longue die Resilienz der gesamten Wirtschaft.

Und zu guter Letzt: auch das Offboarding gehört zur Unternehmenskultur. Es wäre utopisch anzunehmen, dass ständig und überall Zufriedenheit herrscht und man immer im Guten auseinandergehen könnte – wie immer gilt beim Risiko: Es ist nie null, aber meistens doch mitigierbar.

Autoren: Paul André de Jong, Unternehmensberatung Claudia de Jong und Mag. Julia Nusko, B. A., Calpana business consulting

Kontakt:
Unternehmensberatung Claudia de Jong
Diepholz
Paul André de Jong
Tel.: +49 5441/5949927
paul.dejong@dejong.consulting
www.dejong.consulting

Calpana business consulting GmbH
Linz
Mag. Julia Nusko, B.A.
Tel.: +43 732/ 601 216 – 0
julia.nusko@calpana.com
www.calpana.com

Literatur

[1] https://www.focus.de/gesundheit/news/ein-mann-im-krankenhaus-frau-kauft-erdbeeren-als-sie-reinbeissen-will-entdeckt-er-gefaehrlichen-inhalt_id_9577726.html (02.07.2023)
[2] https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends (02.07.2023)