audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Aktuelle IT-Sicherheit Bedrohungslage für Unternehmen

Zusammenfassung

In der heutigen Zeit ist Informationstechnologie aus nahezu allen Berufen und Branchen nicht mehr wegzudenken. Handwerkliche Maschinen werden von Computern gesteuert oder werden sogar selbst zu ihnen. Prozesslandschaften von Unternehmen finden zunehmend digital statt und alles steht still, wenn die IT stillsteht. Doch noch immer sehen viele Menschen Cyber-Angriffe nicht als Bedrohung für das eigene Unternehmen. In diesem Whitepaper fassen wir die Bedrohungslage im Jahr 2020 konkret für Sie zusammen und zeigen auf, wie Cyber-Angriffe heute funktionieren und wie Sie sich und Ihr Unternehmen weitestgehend schützen können, denn Einhundertprozentige Sicherheit existiert bekanntlich nicht.

Problemstellung

IT-Sicherheit ist ein komplexes Thema, welches sich so schnell weiterentwickelt, dass es selbst fachkundigen Menschen mit informationstechnischer Vorbildung schwer fällt Schritt zu halten. Der Einzug von komplexen Cloud-Infrastruktur-Anbietern, dem industriellen Internet der Dinge (IIOT), künstlichen Intelligenzen und einer massiv wachsenden Vernetzung von Hardware, Software und Prozessen gepaart mit datenschutzrechtlichen Anforderungen macht IT-Sicherheit zu einem Sachverhalt, der die Ressourcen eines Unternehmens mitunter schnell verbrauchen kann. Was aber ist das richtige Level oder die richtige Menge an Zeit, Geld und Kapazität von Mitarbeitenden, das Unternehmen zur Verfügung stellen sollten, um einerseits nicht morgen von einer Cyber-Attacke in den Ruin getrieben zu werden, auf der anderen Seite jedoch auch nicht jeden verdienten Euro in IT-Sicherheit zu verbrennen? Diese Frage werden wir, soviel vorab, in diesem Whitepaper nicht beantworten können, allerdings verschaffen wir einen Überblick dessen, worauf sich Unternehmen in diesem und den kommenden Jahren einstellen sollten. Fakt bleibt jedoch, dass IT-Sicherheit noch immer ein unterprivilegiertes und auch unterfinanziertes Thema ist. Denn IT-Sicherheit verdient kein Geld und im besten Fall habe ich als Unternehmen Unsummen investiert und es ist ja doch nichts passiert – zum Glück, wie Unternehmen dann sagen sollten.

Bedrohungen und Abhilfe

In diesem Abschnitt stellen wir zunächst die, unserer Auffassung nach, vier wichtigsten IT-Sicherheitsthemen im Jahr 2020 vor, erläutern warum diese es in die TOP 4 geschafft haben und stellen dar, wie Sie ihr Unternehmen davor schützen können.

Phishing

Phishing (Neologismus von fishing, engl. für ‚Angeln') ist eine Unterform von Social Engineering und verursacht bereits seit Jahren bei Unternehmen den größten Schaden. Angreifer versuchen durch Phishing den Benutzer zu täuschen und diesen dazu zu bringen, sensible Informationen preis zu geben. Das Niveau von Phishing Angriffen hat sich in den letzten Jahren deutlich erhöht. Die Inhalte von Phishing Nachrichten sind nur noch schwer von realen Nachrichten zu unterscheiden und Angreifer nutzen auch moderne Kommunikationsdienste (Instagram, WhatsApp etc.) um noch authentischer zu wirken.

Ein Schutz vor Phishing Angriffen ist aus technischer Sicht nur schwer möglich. Grundsätzlich sollten nur E-Mail-Dienste und Verwaltungsprogramme verwendet werden, welche einen integrierten Schutzfilter bieten und damit weniger professionell entwickelte Phishing Nachrichten blockieren oder den Benutzer auf Auffälligkeiten aufmerksam machen. Solche technischen Schutzmaßnahmen bieten jedoch keinen Schutz gegen fortgeschrittene Phishing Angriffe. Die wichtigste Schutzmaßnahme ist daher die Sensibilisierung der Mitarbeiter. Neben klassischen Schulungsmaßnahmen haben sich insbesondere simulierte Phishing Angriffe als effektives Mittel herausgestellt, um Mitarbeiter das Bedrohungspotenzial zu verdeutlichen.

Schnittstellen

Kaum ein Unternehmen kommt ohne Schnittstellen zwischen dem internen Unternehmensnetzwerk und mobilen Geräten (Laptops, Tablets, Smartphones usw.) aus. Schon vor Ausbruch der COVID-19 Pandemie hatten etwa 39 Prozent[1] der Arbeitnehmer die Möglichkeit auf Homeoffice und Tätigkeiten im Außendienst sind ohne Zugriff auf interne Daten nur schwer möglich. Solche Schnittstellen öffnen zwangsläufig Einfallstore für Angreifer, sind diese nicht entsprechend abgesichert, kann dies schwerwiegende Folgen haben. Erschwerend kommt hinzu, dass eine Kompromittierung der mobilen Geräte der Mitarbeiter gleichzeitig eine Bedrohung für das interne Netzwerk darstellt. Insbesondere bei BYOD Richtlinien kann dies eine zu Problemen führen. Somit müssen sowohl Schnittstellen als auch Endgeräte abgesichert werden.

Die Absicherung von Endgeräten kann sowohl technisch als auch organisatorisch erfolgen. Technisch bieten sich Mobile Device Management (kurz: MDM) Lösungen an, mit dem das Unternehmen mehr Kontrolle über die bereitgestellten Endgeräte hat. Organisatorisch sollten die Mitarbeiter im Rahmen von Schulungen über potenzielle Risiken aufgeklärt werden.

Die Absicherung der Schnittstellen erfolgt zumeist durch eine Auditierung der Schnittstellen-Konfiguration. Insbesondere VPN Lösungen müssen vor potenziellen Angriffen geschützt werden. Neben der Überprüfung der Konfiguration, können auch spezielle Netzwerk Schwachstellen-Analysen durchgeführt werden und damit potenzielle Angriffe simuliert werden. Mithilfe dieser Informationen können die Schwachstellen anschließend beseitigt werden.

Web-Security

Die Website eines Unternehmens ist der öffentliche Auftritt eines Unternehmens und spiegelt dessen Identität wider. Branchenunabhängig findet der erste Kundenkontakt heutzutage primär auf der Website des Unternehmens statt. Die Kompromittierung des Internetauftritts kann schwerwiegende monetäre, reputative und rechtliche Konsequenzen nach sich ziehen. Trotz dieser Risiken ist das Problembewusstsein diesbezüglich bis heute als sehr gering einzustufen, 9 von 10 Websites sind mit einer Vielzahl von Techniken angreifbar.[2]

Der beste Weg, um sich vor virtuellen Angriffen auf die eigene Internetpräsenz zu schützen, ist das Auffinden und Beheben von Schwachstellen. Erst wenn die Probleme identifiziert wurden, können Schutzmaßnahmen getroffen werden.

Cloud-Security

Die Nutzung von Cloud Lösungen steigt stetig, knapp 69% der Unternehmen nutzten im Jahr 2019 bereits hybrid Cloud Lösungen[3] und es wird erwartet, dass bis zum Jahr 2021 ca. 94% der digitalen Arbeitslast in der Cloud stattfinden wird.[4] Dieser Trend ist nachvollziehbar, die Liste der Vorteile enthält, neben vielen weiteren Punkten, Kernaspekte wie Skalierbarkeit, Flexibilität und Kostenreduktion. Leider ist die Liste der Nachteile und potenziellen Risiken ebenfalls sehr lang. Zudem müssen an dieser Stelle auch datenschutzrechtliche Überlegungen berücksichtigt werden. Ein unstrukturierter Umzug in die Cloud kann somit am Ende mehr Kosten als Vorteile bringen.

---

[1] https://www.bitkom.org/Presse/Presseinformation/Vier-von-zehn-Unternehmen-setzen-auf-Homeoffice
[2] https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/
[3] https://451research.com/images/Marketing/press_releases/Pre_Re-Invent_2018_press_release_final_11_22.pdf
[4] https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html

Der beste Weg, um sich vor unvorhergesehen Risiken und Problemen während eines Umzugs in die Cloud zu schützen, ist die genaue Planung des Umzugs, welcher insbesondere auch Sicherheitsaspekte berücksichtigen muss. Nach dem Umzug muss das Personal im Umgang mit der neuen Technologie geschult und die Konfigurationen regelmäßig auditiert werden. Reichen die internen IT-Ressourcen nicht aus, um diese Aspekte sicherzustellen, sollte das Unternehmen sich durch externe Spezialisten unterstützen lassen.

Autor und Ansprechpartner

Sascha Knicker
Senior Consultant Datenschutz und Informationssicherheit

Schwerpunkte: Datenschutz, TISAX, ISO 27001

Mail: s.knicker@audatis.de
Fon: 05221 87292-07

LinkedIn | Twitter | XING

Marcel Albrink
Consultant Informationssicherheit

Schwerpunkte: TISAX, ISO 27001

Mail: m.albrink@audatis.de
Fon: 05221 87292-07

LinkedIn | Twitter | XING

Haben Sie noch Fragen?

Wir haben versucht, alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Wir unterstützen Sie gerne bei der Planung von datenschutzkonformen und sicheren Apps und der Beantwortung aller Fragen in Bezug auf die pragmatische Umsetzung des Datenschutzes und der Informationssicherheit.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de

© Copyright 2020, audatis Consulting GmbH.

Dieses Whitepaper wird Ihnen von der audatis Consulting GmbH zur Verfügung gestellt und darf gerne unverändert weitergegeben oder veröffentlicht werden.