ZeTT-Zentrum
Digitale Transformation
Thüringen

Zukunfts-Zentren

BETRIEBSRISIKO IT-SICHERHEIT
To-do-Liste für KMU

Autoren:

Jan Zipperling, Thomas Engel und Mario Jandeck

BETRIEBSRISIKO IT-SICHERHEIT
To-do-Liste für KMU.

Cyber-Attacken gehören längst zum betrieblichen Alltag und sind Teil der digitalen Normalität. Während die meisten Menschen bei Cyber-Attacken an sensible Infrastruktur, Hackerangriffe auf große Unternehmen und den Diebstahl von Staatsgeheimnissen denken, ist das Risiko für kleine und mittlere Unternehmen (KMU) nicht so präsent. Wie steht es um die Sicherheit und das Gefährdungsrisiko von KMU? Wie leicht werden KMU Opfer einer Cyber-Attacke? Was können KMU vorbeugend unternehmen, um sich zu schützen?
Es gilt mit vielen Irrtümern aufzuräumen und realistische Hilfestellungen anzubieten. Diese Handreichung klärt über typische Irrtümer auf und gibt Hinweise für einen Grundschutz, welchen Verantwortliche in KMU beachten können, um die IT-Sicherheit im Unternehmen zu erhöhen.

Irrtum #1 „Unser Unternehmen ist so klein, da lohnt sich Hacking gar nicht!" Realistische Risiken für KMU erkennen.

Auch wenn das Risiko, Opfer einer aufwändig geplanten Cyber-Attacke zu werden, tatsächlich für KMU verhältnismäßig gering ist, bestehen Risiken für ihre IT-Infrastruktur. So werden beispielsweise Emails verschickt, die den Empfängern Gewinne versprechen, die sich durch Klicken auf einen Link einlösen lassen. Dahinter verbirgt sich in der Regel ein Virus, über den ein externer Zugriff auf Dateien im Rechner ermöglicht wird.
Neben diesen berüchtigten Phishing-Mails gehören weitere Attacken (z.B. sogenannte DDoS-Angriffe) und die Suche nach Schwachstellen in der IT-Infrastruktur durch Bots zu typischen Methoden.

Bei einer Distributed-Denial-of-Service-Attacke (DDoS), wird ein Zielrechner oder Server durch eine Vielzahl infizierter Rechner simultan mit Anfragen belegt, wodurch das IT-Netz überlastet wird und der normale Datenverkehr nicht mehr oder nur verzögert gewährleistet werden kann. Als Bot werden automatisierte Programme bezeichnet, welche selbstständig nach Schwachstellen in der IT von Unternehmen scannen.

Alle genannten Formen von Attacken zeichnen sich durch ihre automatisierte Operationsweise aus. Hinter ihnen sitzen also nicht Hackergruppen, welche gezielte Angriffe gegen bestimmte Unternehmen führen. Es handelt sich um einmal in Gang gesetzte Algorithmen, die wahllos und prinzipiell unbegrenzt skalierbar Angriffe gegen viele Unternehmen gleichzeitig durchführen können. Das schlägt sich auch in der Häufigkeit von Cyber-Attacken nieder.

Je nach Größe eines Unternehmens berichten zwischen 50 % und 65 % der deutschen Unternehmen im vergangenen Jahr Opfer eines Cyber-Angriffs geworden zu sein, wobei die Dunkelziffer weitaus größer sein dürfte (Dreißigacker, Skarczinski & Wollinger 2020).

Irrtum #2: „Das Passwort ist sicher, das verwende ich immer!“: Typische Schwachstellen in der IT-Infrastruktur von KMU ausschalten.

Was die genannten Cyber-Attacken an Quantität aufbieten können (viele simultane Angriffe gegen viele Ziele), büßen sie an Qualität ein. In den meisten Fällen bestehen Cyber-Attacken aus relativ simplen Algorithmen, welche gezielt häufig aufkommende Schwachstellen in der IT-Infrastruktur des Ziels ausnutzen. Zu diesen Schwachstellen zählen neben schwachen bzw. nicht vorhandenen Passwörtern vor allem unzureichend gepatchte Software und ungenügend bzw. nicht verschlüsselte Kommunikation über digitale Geräte.

Während der entstandene Schaden im Mittel etwa 17.000 Euro beträgt, können schwerwiegendere Angriffe Millionenbeträge kosten, zum Verlust wertvoller Patente führen und im Ausnahmefall den Konkurs einzelner Unternehmen nach sich ziehen.v

Hier sind die IT-Beauftragten im Unternehmen ebenso gefragt, wie die Beschäftigten. Es vbedarf einer regelmäßigen Sensibilisierunvg v vvtfür die Relevanz von Verschlüsselung, Passwörtern und Updates und es ist sinnvoll, klare AnsprechpartnerInnen im Betrieb zu benennen. Wichtig ist, dass eine IT-Sicherheitskultur etabliert wird, die für alle Beteiligten transparent ist. An dieser Stelle können Betriebsräte und Datenschutzbeauftragte wichtige Kooperationspartner sein.

Irrtum #3: „Für den Download habe ich keine Zeit!“
Lösungen für eine widerstandsfähige IT-Infrastruktur etablieren.

Lösungsansätze für die genannten Probleme sind meist leichter umzusetzen als gedacht. Die meisten Schwachstellen sind auf nicht erfolgte „IT-Hygiene“ in KMUs zurückzuführen und lassen sich mit wenig technischem Aufwand beheben. Neben der Verwendung von automatisch generierten Passwörtern und verschlüsselten Kommunikationsmethoden, gehört hierzu vor allem das regelmäßige Updaten aller relevanten Patches. Gerne vergessen werden Hersteller-Patches von extern zugekauften Hardware-Komponenten, die ebenfalls eine Sicherheitslücke darstellen können.

Neben dem technischen Allgemeinwissen, bedarf es der Schulung und Aufklärung von MitarbeiterInnen. Worauf gilt es bei der Verwendung von Software zu achten? Wen kann ich ansprechen, wenn etwas auffällig ist? Diese Fragen erfordern ein Betriebsklima, in dem der Umgang mit Daten und dem IT-System kooperativ und transparent geregelt ist und MitarbeiterInnen ermutigt werden, selbstbewusst mit den vorhandenen IT-Systemen umzugehen. Betriebsvereinbarungen können eine Möglichkeit darstellen, um Themen wie Umgang mit IT-Systemen, Datenschutz und „IT-Hygiene“ verbindlich zu regeln.

Irrtum #4„Damit wäre ja alles erledigt!“ Vorbeugende Maßnahmen einer guten „IT-Hygiene“ vermitteln.

Das Risiko von Cyber-Attacken ist damit nicht einfach erledigt. Eine erfolgreiche IT-Sicherheitsstrategie ist als Prozess zu verstehen, welcher fortlaufend auf den neusten Stand gebracht werden muss. Um diesen Prozess zu erleichtern, ist es in erster Linie notwendig, die Belegschaft in diesen einzubeziehen. Es geht weniger um hochkomplexe technische Zusammenhänge, als vielmehr darum, mittels Schulungen und Workshops MitarbeiterInnen in ihren Kompetenzen im Umgang mit ungewöhnlichem Verhalten der IT im Unternehmen zu stärken.
So wird die Belegschaft befähigt, adäquat auf verdächtige Emails, plötzliche Leistungsverluste der Hardware und Ähnliches zu reagieren und diese Phänomene an IT-Sachverständige rückzumelden.

Im besten Fall wird Angriffen präventiv begegnet oder diese zumindest so früh erkannt, dass keine ernsthaften Schäden entstehen.

Haben Sie Fragen? Wer kann helfen?
ZeTT unterstützt Sie gerne dabei, geeignete Ansprechpartner für Ihre IT-Sicherheitsfragen zu finden. Das Unternehmen Enginsight, das das ZeTT bei der Erstellung dieser Checkliste beraten hat, ist beispielsweise ein geeigneter Partner zur Überprüfung ihrer IT-Sicherheitskultur. Zu weiteren ExpertInnen auf dem Gebiet der IT-Sicherheit gehören u.A.: ASOFTNET (Erfurt), CODA GmbH (Erfurt), FUTUREDAT (Gera), ESET (Bratislava).

Für weitere Fragen stehen wir ihnen selbstverständlich zur Verfügung. Kontaktieren sie uns ganz einfach per Mail oder Telefon.

CHECKLISTE IT-SICHERHEIT:

- [ ] **Realistische Risiken für KMU erkennen (Seite 3)**
- [ ] **Typische Schwachstellen in der IT-Infrastruktur von KMU ausschalten (Seite 4)**
- [ ] **Lösungen für eine widerstandsfähige IT-Infrastruktur etablieren (Seite 5)**
- [ ] **Vorbeugende Maßnahmen einer guten „IT-Hygiene“ vermitteln (Seite 6)**
- [ ] **Automatisierte Passwörter einrichten**
- [ ] **Kommunikation verschlüsseln**
- [ ] **Aktuelle Patches und Updates durchführen**
- [ ] **Schulung von Mitarbeiter:innen zum Thema IT-Sicherheit durchführen**
- [ ] **IT-Verantwortliche im Unternehmen identifizieren**

FRIEDRICH-SCHILLER-UNIVERSITÄT JENA

Ernst-Abbe-Hochschule Jena
University of Applied Sciences

Arbeit und Leben Thüringen DGB/VHS

TECHNISCHE UNIVERSITÄT ILMENAU

IHK Erfurt

ZeTT – Zentrum
Digitale Transformation
Thüringen

Bachstraße 18k|07743 Jena
+49 (0)123/45 67 89-0
c.schickert@zett-thueringen.de
www.zett-thueringen.de

Das Projekt „ZeTT–Zentrum Digitale Transformation Thüringen" wird im Rahmen der Förderrichtlinie „Zukunftszentren – Unterstützung von KMU, Beschäftigten und Selbständigen bei der Entwicklung und Umsetzung innovativer Gestaltungsansätze zur Bewältigung der digitalen Transformation" durch das Bundesministerium für Arbeit und Soziales und den Europäischen Sozialfonds gefördert.

Gefördert durch:

Bundesministerium für Arbeit und Soziales

Kofinanziert von der Europäischen Union

Weiterer Förderer:

Freistaat Thüringen
Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie