Zum Tag der Computersicherheit

von ASCONSIT | Veröffentlicht am 30. November 2021



Wann und wo beginnt Computersicherheit?

Heute ist der Tag der Computersicherheit! Aber was hat es mit diesem Tag eigentlich genau auf sich?

Zunächst fällt eine etwas veraltete Begrifflichkeit auf. Dass kommt daher, dass der Tag der Computersicherheit bereits 1988 von der US-amerikanischen „Association for Computer Security“ (Vereinigung zur Computersicherheit) ins Leben gerufen wurde mit dem Ziel, die Awareness für das Thema zu steigern. Seitdem feiern wir jedes Jahr am 30. November den Tag der Computersicherheit. Denn auch, wenn der Begriff ein wenig altbacken wirkt und wir heute eher von IT-Sicherheit sprechen, die Problematik ist aktueller denn je.

IT und IT-Sicherheit sind heutzutage zentrale Bestandteile eines jeden Unternehmens und bilden die Basis für nahezu alle Geschäftsprozesse. Bei IT-Störungen kann das im schlimmsten Fall den gesamten Betrieb oder auch die Produktion zum Stillstand bringen, was großen wirtschaftlichen Schaden verursachen kann. Aus diesem Grund sollten Unternehmen ihre IT-Systeme absichern und gegen existierende Risiken und Angriffsmöglichkeiten schützen. Systemausfälle und Datenmanipulation gilt es zu verhindern.

Aber wo genau beginnt denn Computersicherheit? Bei der Planung der Netzwerkstruktur, der Auswahl der richtigen Hard- und Softwarekomponenten, in den Köpfen der Mitarbeiter oder bei der Anmeldung am System? Tatsache ist: Computersicherheit ist komplex und umfasst zahlreiche Faktoren wie beispielsweise:

- Netzwerksicherheit
- Datensicherung, Datenschutz und Datenverschlüsselung
- Betriebssysteme und Software (inkl. Updates und Sicherheitspatches)
- Einbindung von Remote-Arbeitsplätzen und mobile Endgeräten
- Anmeldeprozesse und Berechtigungen der Mitarbeiter und Externen

Unbestritten ist außerdem, dass sich die gesamte Technologie seit dem Ende der 1980er Jahre rasant weiterentwickelt hat und es kommen regelmäßig neue Bedrohungsarten hinzu, denn Cyberkriminelle entwickeln kontinuierlich neue Angriffsmethoden. Inzwischen sind sie meist professionell organisiert und arbeiten mit modernster Technik. Der Umsatz ist mittlerweile größer als beim Drogenhandel. IT-Sicherheit ist also ein ständiger Wettlauf mit den wachsenden Bedrohungen. Häufige Angriffsmethoden sind:

- Advanced Persistent Threats (APTs)
- Schadsoftware/Malware
- Ransomware
- Spam und Phishing
- Botnetze

Am Beginn von IT-Sicherheit steht eine ausführliche Analyse

Wichtig ist, sich in diesem Zusammenhang zu vergegenwärtigen, dass IT-Sicherheit und Cybersecurity nicht nur eine Frage der Technik sind. Denn tatsächlich ist der Mensch bzw. der Mitarbeiter eine der größten Schwachstellen im System. Um IT-Risiken zu minimieren und eine möglichst umfassende IT-Sicherheit zu gewährleisten, müssen Unternehmen also sowohl technische als auch organisatorische Maßnahmen ergreifen. Zu Beginn sollte eine ausführliche Prozess- und Schwachstellenanalyse durchgeführt werden. Sie hilft festzustellen, welches genau die geschäftskritischen Prozesse sind, ob sie Schwachstellen haben, wie groß das Risiko ist, dass diese Schwachstellen ausgenutzt werden und welchen Schaden dies konkret anrichten kann. Alle IT-Risiken auszumerzen, wird kaum gelingen, aber vorhandene Risiken sollten im Hinblick auf ihre Bedeutung klar kategorisiert und möglichst aktiv gemanagt werden, während gleichzeitig die Belegschaft für das Thema IT-Sicherheit sensibilisiert wird.

Wir von ASCONSIT unterstützen Sie gerne bei der Analyse Ihrer Geschäftsprozesse unter IT-Sicherheitsaspekten und sind darüber hinaus auf professionelles Identity & Governance & Access

Management spezialisiert. In Zeiten des digitalen Wandels zählt es zu den kritischen Erfolgsfaktoren eines Unternehmens und ist essentieller Bestandteil einer durchdachten und fundierten IT-Sicherheitsstrategie.

Sie möchten gerne mehr über uns und unsere Leistungen erfahren? Dann nehmen Sie gerne Kontakt zu uns auf. Wir freuen uns auf den Austausch mit Ihnen!