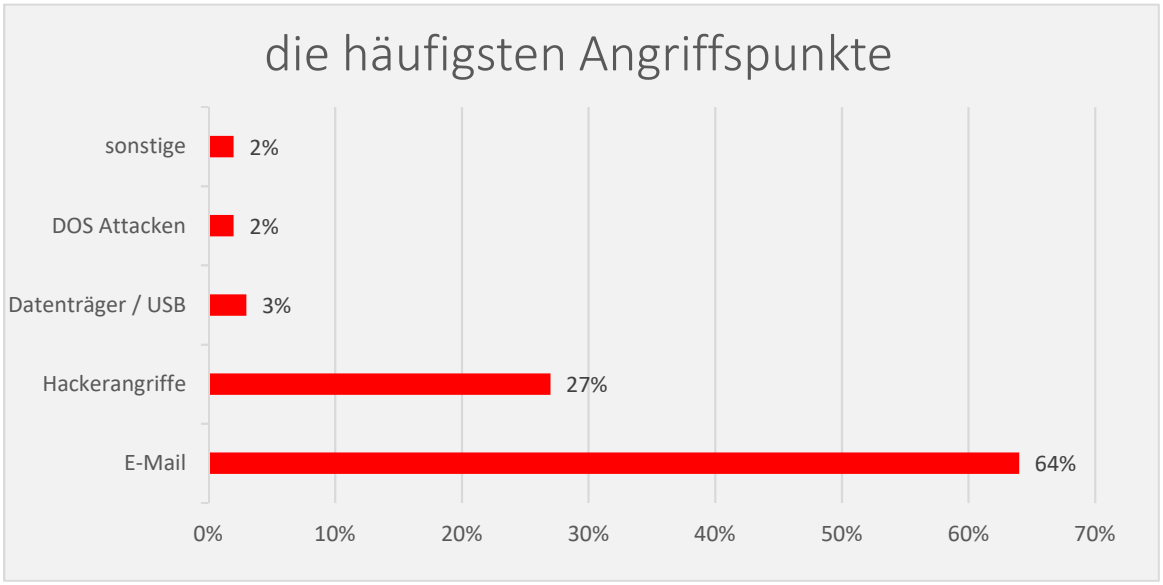
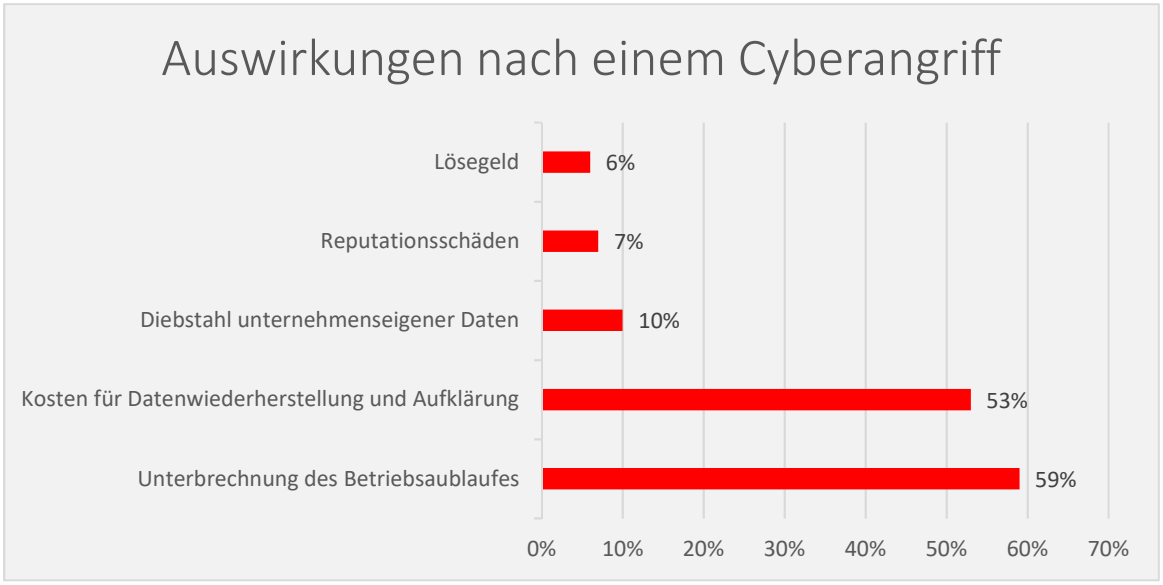
Internet & Cyberrisiken

„EDV“ - Ende der Vernunft?

Eher nicht, aber die zunehmende und notwendige Vernetzung im und zwischen den Unternehmen birgt auch die Gefahr der totalen Abhängigkeit. Weil: „nichts geht mehr ohne EDV“. Das BKA sowie der IT-Branchenverband „Bitkom“ haben Schäden durch Hacker in der deutschen Wirtschaft allein für 2019 auf ca. 103 Mrd. Euro beziffert. Und der Trend zur Kriminalität geht weiter. Das BSI zählt binnen eines Jahres mehr als **117 Millionen** neue Schadprogramme. Das sind 320.000 pro Tag.





Quelle: GdV (Gesamtverband der deutschen Versicherungswirtschaft)

Oftmals vorgebrachte Einwände

„*man sei als Unternehmen zu klein, zu uninteressant*“

Das ist den Hackern ziemlich egal. Großunternehmen sind sicher interessanter und lukrativer, aber auch anspruchsvoller. Und dennoch, gerade Unternehmen bei denen vermutlich eine eigene IT- Mannschaft rund um die Uhr zur Verfügung steht und finanzielle Mittel „keine Rolle“ spielen, werden gehackt. Bei allen anderen wird nach dem Gießkannenprinzip vorgegangen, gleichgültig wenn es trifft. Entweder aus Spaß, weil man „es kann“, oder um durch Erpressung an schnelles Geld zu kommen.

„*die Daten liegen in einer Cloud und sind somit sicher*“

Ein Cloudanbieter verarbeitet bzw. sichert Computerdaten. Er haftet aber weder für deren Inhalt noch für vermeintliche DSVGO Verstöße des Kunden. Werden Daten abgegriffen, missbraucht, schadhafte Programme geladen, Daten intern oder extern manipuliert, wird ein Cloudanbieter weder in einen Rechtsstreit für seinen Kunden noch für dessen Folgekosten aus einer Datenmanipulation aufkommen.

„*Hacker müssen über besondere Fähigkeiten verfügen*“

Leider nein. Sinnigerweise kann über „Webshops“ die Schadsoftware bezogen werden. Es gibt leider nichts, was man im Internet (legal oder nicht), nicht besorgen könnte.

„*mein System ist sicher“ und wird regelmäßig durch eine interne-/ externe IT-Firma / Administrator aktualisiert*“

Die vorrangige Aufgabe eines Administrators wird sein, dass das EDV-System (egal wie) schnellstens wieder funktioniert. Kann aber sichergestellt werden, dass ein Virus auf Dauer entfernt werden konnte? Wie groß ist die zeitliche Komponente bei der Fehleranalyse. Sind technisches Equipment sowie fachliches Knowhow vorhanden, um tief in die Systemanalyse einzusteigen, den Fehler zu lokalisieren, zu beheben und das System für zukünftige Angriffe sicher zu machen? Auch eine IT-Firma / Admin arbeitet nicht umsonst. Abgesehen von den Kosten einer Betriebsunterbrechung, von Reputationskosten, Anwaltsgebühren, usw. Hierfür ist weder ein Administrator noch eine IT-Firma „zuständig“.

Unsere laufend aktualisierten Schadeninformationen sprechen für sich !