M&T Metallhandwerk

Vermeiden Sie Datenspionage und die Folgen

Firmendaten werden der genannten Bitkom-Umfrage zufolge nicht nur durch Hackerangriffe über Internet gestohlen, sondern etwa zu einem Drittel physisch durch den Diebstahl von Datenträgern, IT- und Kommunikationsgeräten. In weiteren rund zwanzig Prozent der Fälle erfolgt die Ausspähung durch den Diebstahl digitaler Dokumente. In einem ähnlichen Umfang kommt es in den Unternehmen zu Sabotageakten, mit dem Ziel, betriebliche Abläufe zu stören oder lahmzulegen. Das kann zu Zeitverlusten im Betriebsablauf führen, bei Produktionsanlagen Schäden verursachen oder die Produktqualität mindern. In einigen Fällen wurden der Umfrage zufolge auch Mitarbeiter durch unterschiedliche Maßnahmen beeinflusst, vertrauliche Informationen wie Passwörter unbewusst preiszugeben. Bei weiteren Unternehmen wurde die elektronische Kommunikation ausgespäht oder Telefonate abgehört. Einen großen Teil der daraus resultierenden Schäden machen Umsatzverluste durch Plagiate oder Patentrechtsverletzungen aus, gefolgt von Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen. Ausgaben für die Ersatzbeschaffung gestohlener IT- und Kommunikationsdaten sowie durch den Ausfall von IT-Systemen oder die Störung von Betriebsabläufen entstehende Kosten sind weitere Schäden. Nicht zu unterschätzen sind auch als Folge von Sicherheitsvorfällen eintretende Imageschäden. Erstaunlich ist, dass gemäß Umfrage in den meisten Fällen eigene Mitarbeiter die Täter sind: In fast zwei Drittel der betroffenen Unternehmen waren aktuelle oder ehemals Beschäftigte für die Taten verantwortlich. Bei einem Drittel der Befragten kamen die Angriffe aus dem unmittelbaren Umfeld von Kunden, Lieferanten oder Dienstleistern. Wettbewerber waren der Bitkom-Umfrage zufolge bei 16 Prozent der befragten Unternehmen für die Taten verantwortlich, weitere zwanzig Prozent kamen aus dem Umfeld organisierter Banden oder ausländischer Geheimdienste.

Das haben die Kunden davon …

Virenschutz ist auch Kundenschutz. Schließlich kann man selbst schnell zur Viren-Schleuder werden: Ein per E-Mail-Anhang als DOC- oder PDF-Datei versandtes Angebot kann die Rechner von Kunden infizieren, wenn sich unbemerkt ein Virus einnistet. Das kann nicht nur dazu führen, dass man Kunden in Schwierigkeiten bringt, sondern auch, dass Geschäftsbeziehungen beendet werden. Eigene E-Mail-Anhänge sollten deshalb vor dem Versand automatisch durch entsprechende Programme auf mögliche Schadsoftware untersucht werden.

Weitere Infos/Quellen

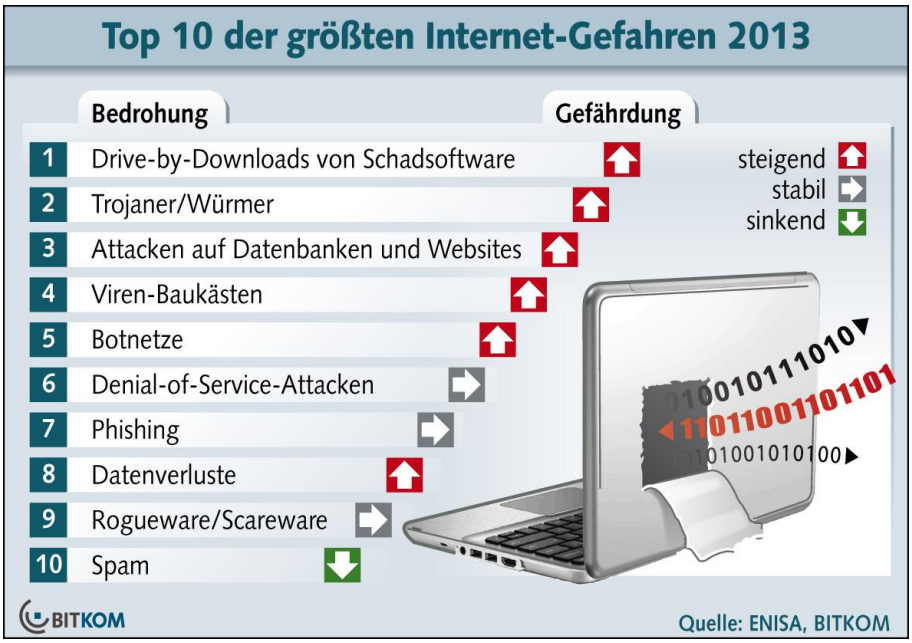
- BMWi, Netzwerk Elektronischer Geschäftverkehr (Hrsg.): IT-Sicherheit: Themenfokus Sicheres Mobiles Arbeiten, Köln 2012, Download: www.mittelstand-digital.de/DE/wissenspool,did=525618.html,
- www.avira.com/de/threats: Aktuelle Virenübersicht,
- www.bitkom-datenschutz.de: Datenschutz-Infos der Bitkom,

Coleman
Ein Unternehmen der Gruppe Rudolf Müller

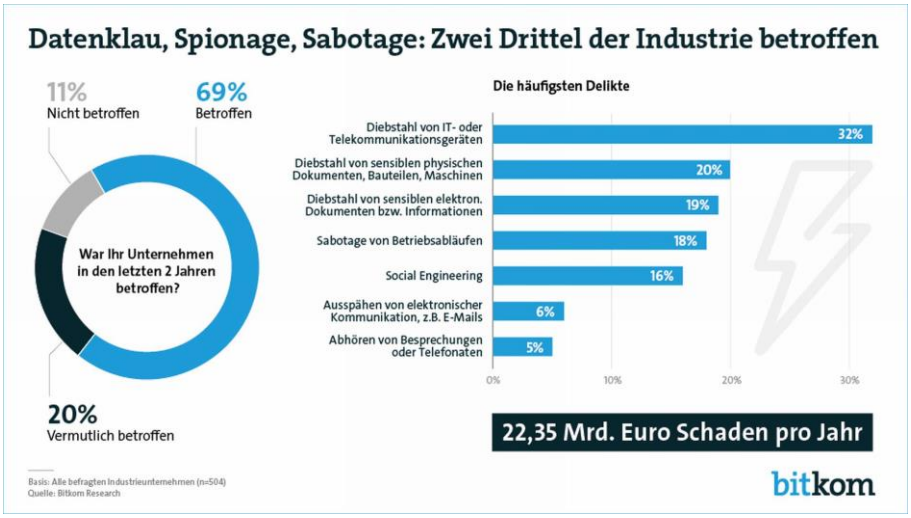
M&T Metallhandwerk

- www.bsi.bund.de: Bundesamt für Sicherheit in der Informationstechnik,
- www.mittelstand-digital.de: Wissenspool, IT-Sicherheit für KMU,
- www.heise.de/security: Security-Portal Heise-Verlag,
- www.virenschutz.info: Virenschutz-Info-Portal,
- www.wikipedia.de: Suche: Internetkriminalität etc.

(Auswahl ohne Anspruch auf Vollständigkeit)



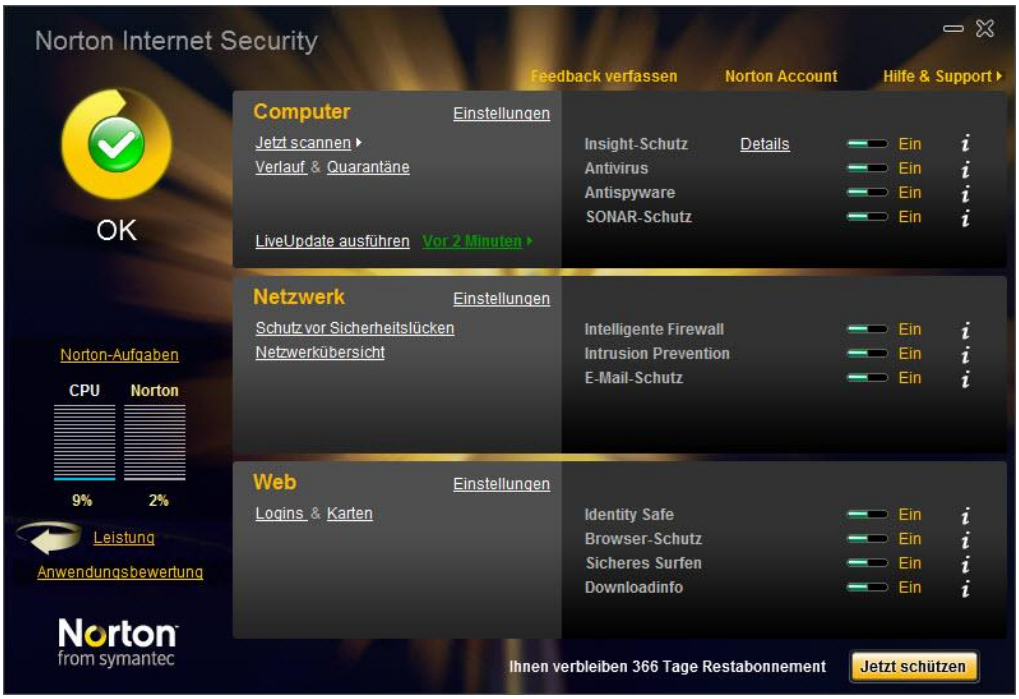
Waren vor wenigen Jahren vor allem Schadprogramme ein wichtiges IT-Sicherheitsthema,…
Grafik: Bitkom



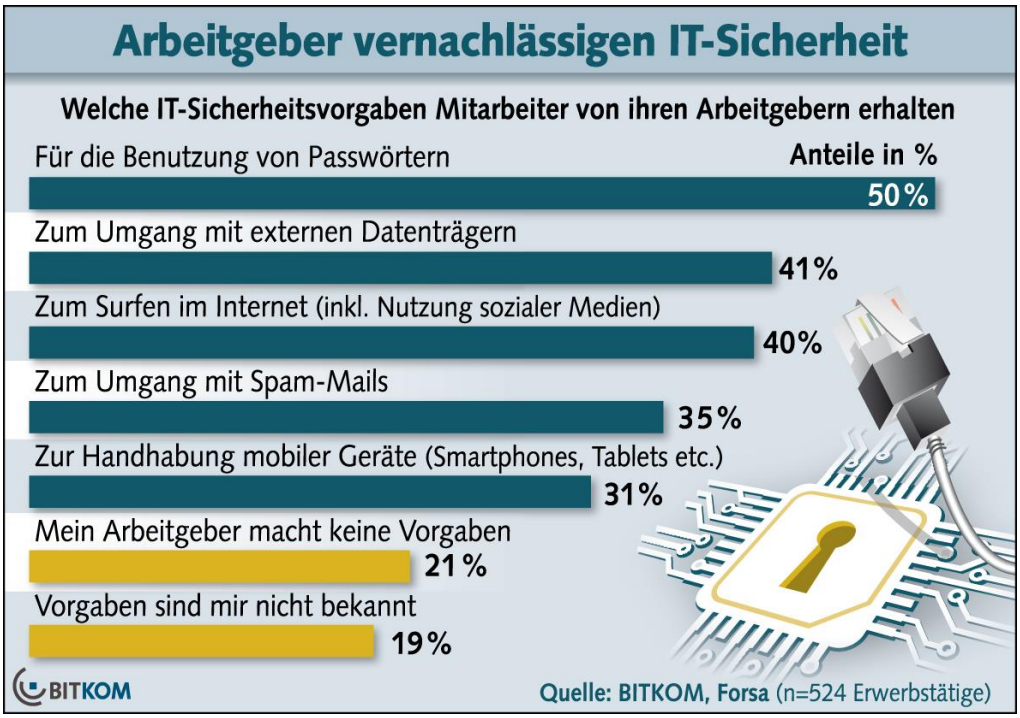
… sind heute Untersuchungen zufolge zunehmend auch der Datenklau, Spionage- und Sabotageaktivitäten ein Problem.
Grafik: Bitkom

Coleman
Ein Unternehmen der Gruppe Rudolf Müller

M&T Metallhandwerk



Mit Antiviren-Software und anderen Sicherheitsmaßnahmen kann man sich davor schützen.
Screenshot: Symantec



Auch die Mitarbeiter müssen über Schulungen und Sicherheitsvorgaben in das IT-Sicherheitskonzept eingebunden werden.
Grafik: Bitkom

Coleman
Ein Unternehmen der Gruppe Rudolf Müller