Cyber Versicherung - Hackerangriffe

Wie ein Cyberangriff das Unternehmen erschüttert & wie man sich davor schützen kann!

fashionconsult

Cyberangriffe nehmen zu!

Unternehmen Teilen Merken

IT-SICHERHEIT

Großkonzerne hilflos gegenüber Hackern

VON STEPHAN FINSTERBUSCH - AKTUALISIERT AM 08.11.2021 - 18:41

Die Hacker haben die Systeme der Handelskette MediaMarktSaturn gekapert und bis auf weiteres Daten eingefroren. Seit Ausbruch der Corona-Krise sind Unternehmen vermehrt Ziele solcher Angriffe.

Cyberangriffe nehmen zu!

HACKERANGRIFF

Erste Cyber-Katastrophenfall in Deutschland – Landkreis lahmgelegt

Ein Hackerangriff auf Anhalt-Bitterfeld hat den ersten Cyber-Katastrophenfall ausgelöst. Sicherheitskreise vermuten, dass es sich um eine Erpressung handele.

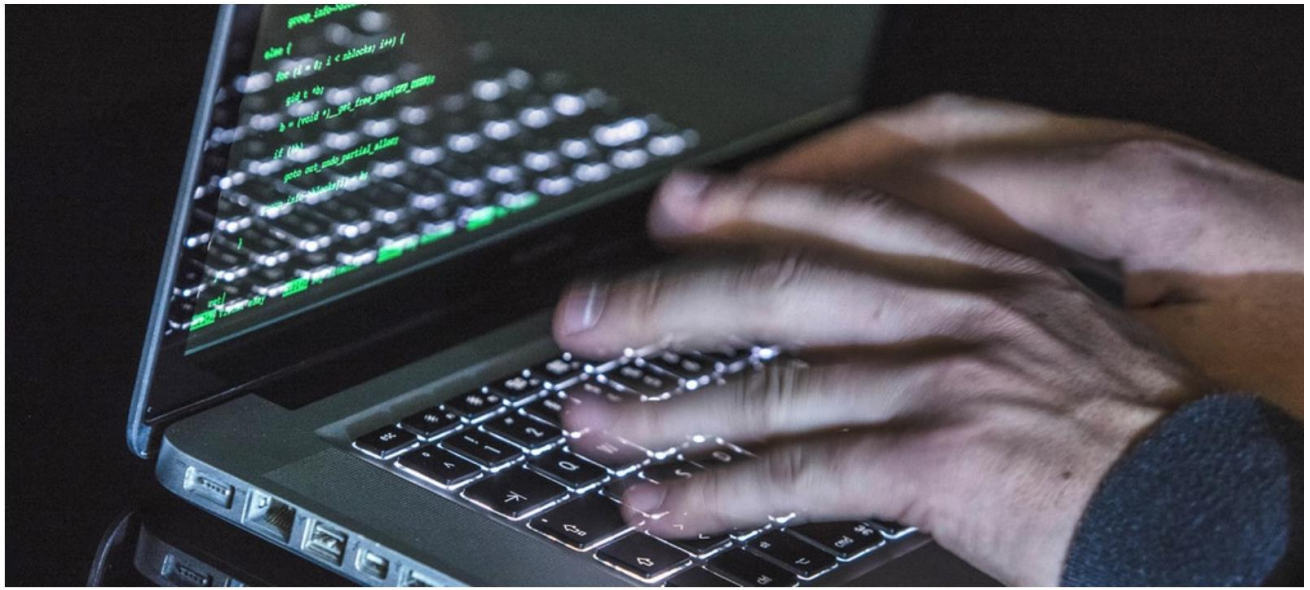
10.07.2021 - 15:23 Uhr • Handelsblatt

Cyberangriffe nehmen zu!

tagesschau

Sendung verpasst?

Wirtschaft ▸ Unternehmen ▸ Nach Cyberangriff: Coop schließt kurzfristig Filialen in Schweden



Nach Cyberangriff

Coop schließt kurzfristig Filialen in Schweden

Stand: 03.07.2021 20:36 Uhr

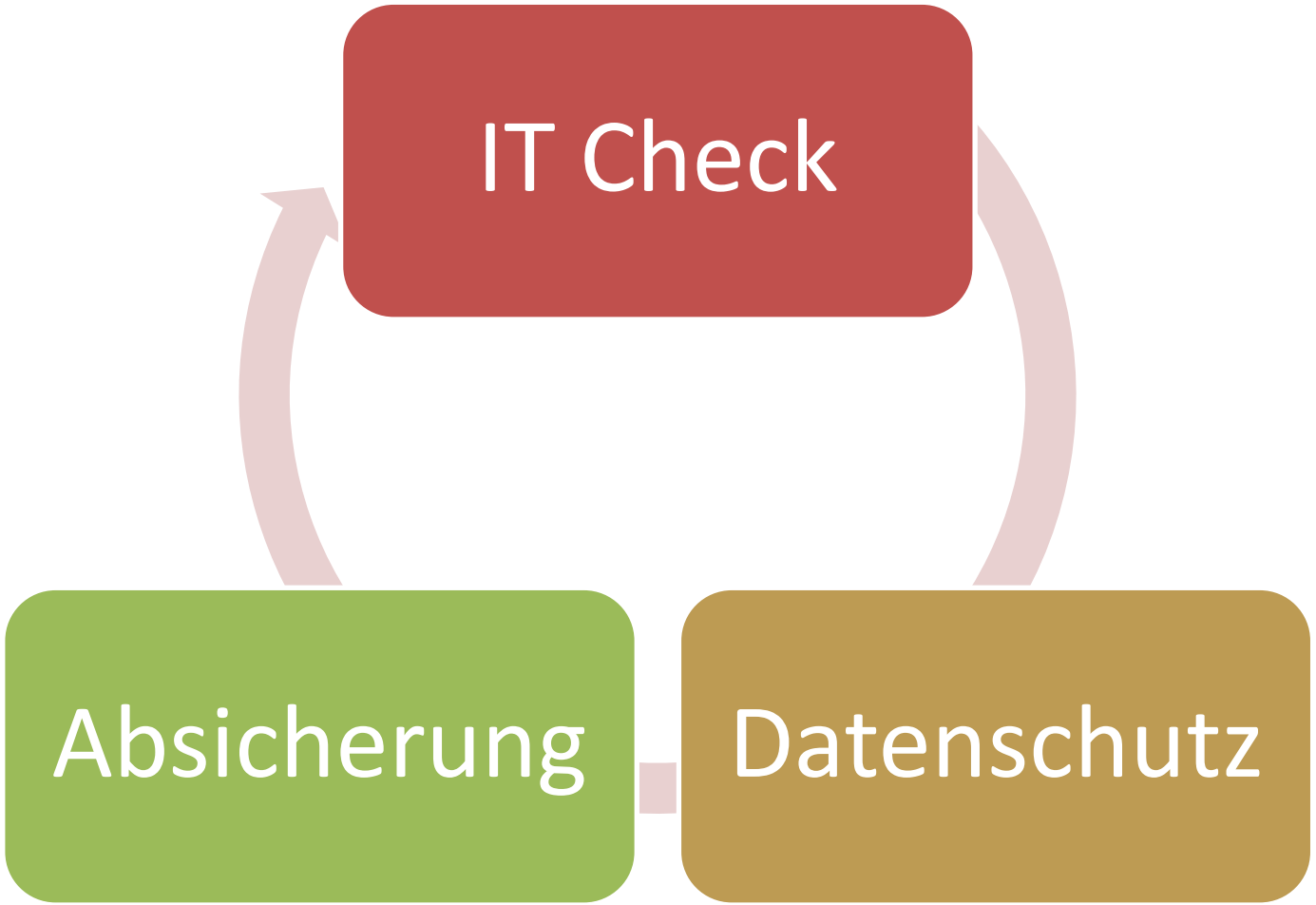
Ein groß angelegter Hackerangriff auf Hunderte Firmennetzwerke in den USA zieht Kreise bis nach Europa. In Schweden waren die Kassen aller Coop-Filialen blockiert, die mit der attackierten Software gesteuert werden.

Hart – aber Real: Andreas Weber berichtet

Für viele von uns war es nur eine Tagesschau-Meldung. Ein Cyber-Angriff hat alle Kassen bei COOP in Schweden lahm gelegt. Für **Andreas Weber** von **Echter** in Murnau und Weilheim war es bittere Realität.

Mehr Angriffe durch CORONA!!

- **Mehr Homeoffice**: Die Verlagerung der Arbeit ins Homeoffice zeigt die Schwachstellen der Systeme auf.
- Der Branchenverband **Bitkom** hat den **Schaden** der **Cyberangriffe** allein für die deutsche Wirtschaft auf **220 Milliarden Euro** p.a. veranschlagt. Das ist eine **Verdoppelung seit Corona**!
- **80 %** aller Groß-Unternehmen weltweit, haben ihre Cyber-Sicherheits-Budgets in den vergangenen Monaten **massiv aufgestockt**. Doch **die Welle** der Angriffe **rollt** ungebremst **weiter**


IT Check
Datenschutz
Absicherung

IT-Check: Das muss beachtet werden!

IT Check

- **Belastbarkeit**
  - Wie widerstandsfähig sind die Systeme bei Sicherheitsvorfällen?
- **Berechtigungskonzept**
  - Zugriffsregeln einzelner Benutzer.
- **Datensicherung**
  - Personenbezogene Daten müssen gegen Verlust geschützt werden.
- **Integrität Zugangsberechtigungen**
  - Mehr-Faktor-Authentifizierung & VPN Zugang – aber richtig!
- **Löschkonzept**
  - Die DSGVO schreibt vor, wann die Daten eines Betroffenen zu löschen sind.

IT-Check: Das muss beachtet werden!

IT Check

- **Altgeräte- Entsorgung**
  - Hardware wird entsorgt – Speichermedien unbedingt zerstören oder professionell löschen!
- **Pseudonymisierung**
  - Daten dürfen betroffene Personen nicht zuordnen lassen
- **Betriebsvereinbarung**
  - Homeoffice mit privaten Endgeräten muss schriftlich geregelt sein
- **Verfügbarkeit gewährleisten**
  - Backups erstellen, Betriebssystem, auch bei Subsystemen, **aktuell** halten, uvm.
- **Verschlüsselung**
  - Alle Möglichkeiten des Betriebssystems ausnutzen

DSGVO Verstoß kann teuer werden!

Datenschutz

ARTIKEL

H&M HAT EINE ENTSCHEIDUNG DER HAMBURGER DATENSCHUTZBEHÖRDE ERHALTEN

H&M: 35 Mio.

1 OKT, 2020

Im Oktober 2019 entdeckte H&M in seinem Nürnberger Servicezentrum eine lokale Sicherheitsverletzung im Zusammenhang mit personenbezogenen Mitarbeiterdaten und meldete diese unverzüglich der Datenschutzbehörde in Hamburg. H&M hat während des Prozesses uneingeschränkt mit der Behörde zusammengearbeitet.

Der Vorfall offenbarte Praktiken bei der Verarbeitung von Mitarbeiterdaten im Servicecenter Nürnberg, die mit den Richtlinien und Anweisungen von H&M nicht vereinbar waren. H&M übernimmt die volle Verantwortung und möchte den Nürnberger Mitarbeitern eine vorbehaltlose Entschuldigung aussprechen.

H&M hat eine Entscheidung von der Hamburger Datenschutzbehörde erhalten, mit der ein Bußgeld in Höhe von 35 Mio. Euro verhängt wird. Das Unternehmen wird diesen Beschluss nun sorgfältig prüfen.

Nach der Aufdeckung und Meldung des Vorfalls leitete H&M im Nürnberger Servicecenter unverzüglich weitreichende Maßnahmen ein. Zur Verbesserung wurde einen umfassenden Aktionsplan aufgelegt zur Verbesserung der internen Audit-Praktiken, um die Einhaltung der Datenschutzbestimmungen zu gewährleisten und um das Wissen der Führungskräfte für die Sicherstellung eines sicheren und datenschutzkonformen Arbeitsumfeldes zu stärken, sowie zusätzliche Schulungen von Mitarbeitern und Führungskräften in diesem Bereich.

Datenschutz

Beispiele: Diese Fragen sollten Sie Ihrem Datenschutzbeauftragten beantworten können:

*Auszug aus dem jährlichen DSGVO Check von fashionconsult…

- Können Sie ein Löschungskonzept vorlegen und so ggf. nachweisen, dass personenbezogene Daten bei Auftragnehmern gelöscht werden?
- Übermitteln Sie Daten an Drittländer z.B. Hosting Homepage?
- Konzept Datenpanne: Gibt es im Falle einer unbefugten Kenntnisnahme durch Dritte von Daten, die nach § 42a BDSG geschützt sind, einen Ablaufplan?
- Wann haben Ihre Mitarbeiter die letzte Datenschutzschulung erhalten?
- Sind alle Zugänge zu Software und IT-Arbeitsplätzen bzw. Kassen mit Benutzererkennung + Passwörtern geschützt?
- Sind alle externen Zugänge ausreichend gesichert z.B. über VPN Lösungen?
- Datensicherungskonzept: Gibt es aktuelle Datensicherungen der wichtigsten Geräte?

Datenschutz

Datenschutz ist Chefsache und benötigt professionelle externe Berater!

- Unternehmen benötigen einen Datenschutzbeauftragten! (extern/intern)
- Sicherheit Ihrer Daten vor Missbrauch / Diebstahl
- Handlungsempfehlungen für den sicheren Umgang mit Daten
- Vermeidung von Rechtsstreitigkeiten
- Vermeidung von Bußgeldern
- Ext. Datenschutzbeauftragter: fc in Kooperation mit KATAG

Absicherung

Wie funktioniert der Versicherungsschutz?

- Fragebogen als Audit/Risikoprüfung, ob eine„Mindestsicherheit“ der IT vorhanden, um ein verbindliches Angebot zu erhalten
- Prämie richtet sich nach der Versicherungs-summe, die an einem möglichen Schaden orientieren sollte
- Versicherungsmakler begleitet den Prozess der Ausschreibung und hilft bei der Wahl des passenden Versicherers

Wichtige Bausteine der Cyber-Risk-Versicherung:

- Forensiker stehen im Krisenfall per Hotline zur Verfügung und helfen auch bei der Prävention vor einem Schaden, z. B. durch Mitarbeiter-schulung
- Ersatz oder Reparatur von beschädigter Hardware
- Wiederherstellung von beschädigter Software
- Ersatz des Ausfallschadens
- Schutz vor Ansprüchen Dritter, z.B. nach Datendiebstahl von Kunden und Mitarbeitern

* fashionconsult hat gute Erfahrungen mit dem KATAG Versicherungsdienst. Ansprechpartner: Axel Wieczorek +49 171 3690437

Ihre Ansprechpartner

Wenn Sie professionelle Datenschutz-Experten suchen, ist fashionconsult Ihr Partner

Sie haben Interesse?

fashionconsult
Lasbeck 18
48329 Havixbeck
Fon: +49 2507 9822700
datenschutz@fashionconsult.de

Ansprechpartner

Leo Faltmann
Fon: +49 2507 9822700