iwd

Der Informationsdienst
des Instituts der deutschen Wirtschaft

Europäische Union | 08.05.2019 | Lesezeit 2 Min.

Cyberkriminalität: Gefährlicher als Panzer

Im Sekundentakt greifen Hacker Unternehmen und Institutionen in der EU an und verursachen Schäden in Milliardenhöhe. Nur gemeinsam können sich die Mitgliedsstaaten gegen die wachsende Gefahr aus dem Netz wehren. Neue Beschlüsse auf EU-Ebene sollen dazu beitragen.

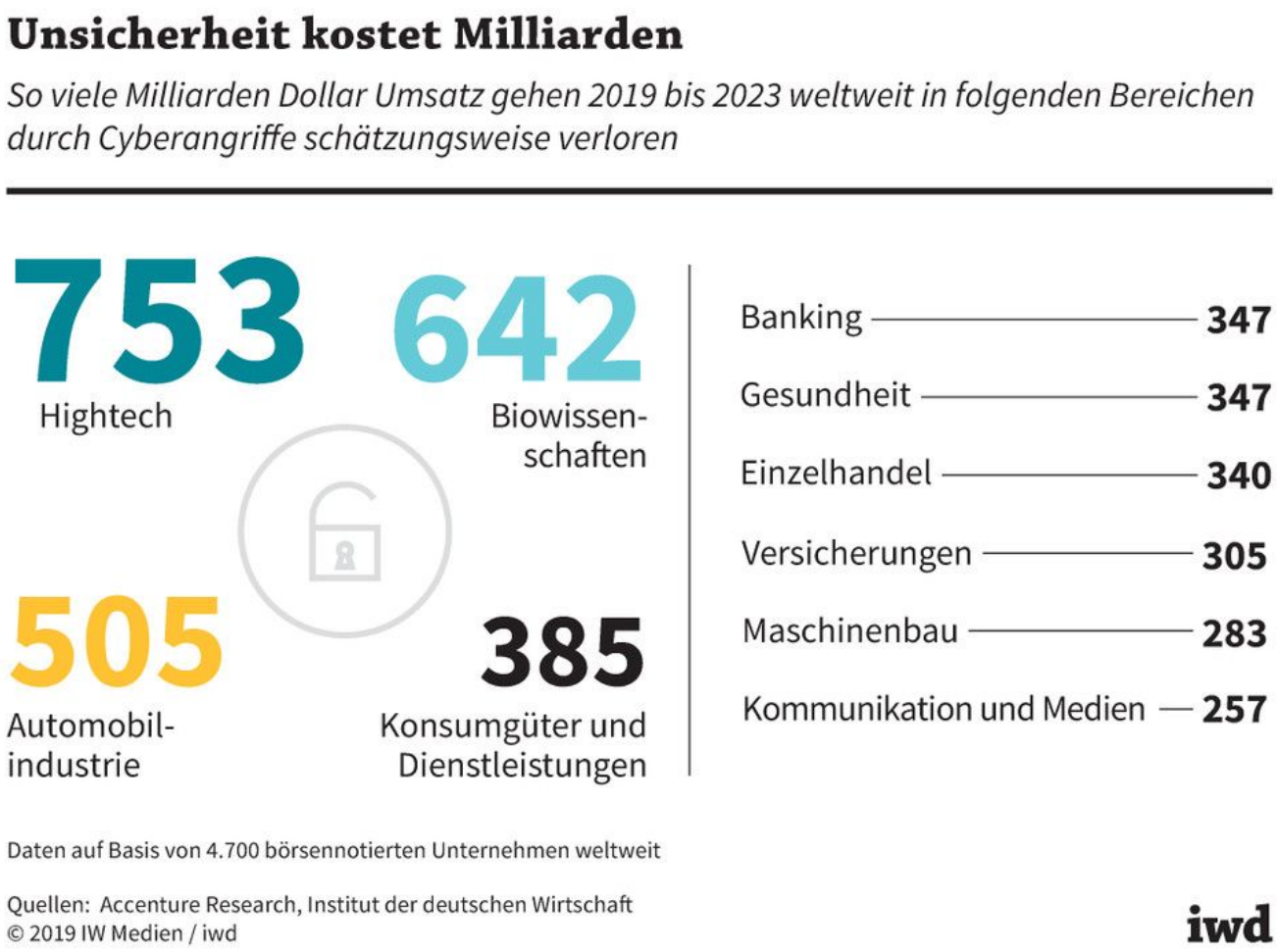
Der Strom fällt aus, Betriebe stehen still, der Verkehr bricht zusammen: Cyberangriffe können dramatische Auswirkungen auf Wirtschaft und Gesellschaft haben. Besonders anfällig ist die Europäische Union mit ihren eng vernetzten Mitgliedsstaaten:

17 EU-Länder hatten seit 2004 mit Wahlmanipulationen via Internet zu kämpfen.

In acht von zehn europäischen Unternehmen kommt es jedes Jahr mindestens zu einem Vorfall, der die Cybersicherheit betrifft.

Rund 500 Milliarden Dollar Schaden verursachen Hackerangriffe jedes Jahr weltweit. Besonders betroffen ist der Hightech-Sektor (Grafik):

Unternehmen wie IBM oder SAP entgehen in den kommenden fünf Jahren voraussichtlich insgesamt 750 Milliarden Dollar Umsatz durch Cyberattacken.



Der Präsident der Europäischen Kommission, Jean-Claude Juncker, sagte in seiner Rede zur Lage der Union 2017: „Cyberangriffe können unter Umständen gefährlicher sein für die Stabilität von Staaten und Unternehmen als Panzer und Gewehre.“ Doch einen Staatenverbund wie die EU zu schützen, ist besonders schwierig. Denn der Kampf gegen die Cyberkriminalität ist ungleich: Ein Hacker muss nur ein kleines Schlupfloch finden, um durch dieses ein riesiges Netzwerk zu infiltrieren. Auf diese Gefahr muss die EU vorbereitet sein.

Das EU-Parlament hat beschlossen, das digitale Immunsystem der Union durch ein – noch zu gründendes – Kompetenzzentrum für Cybersicherheit sowie ein Netz nationaler Koordinierungsstellen zu stärken.

Im April dieses Jahres hat das EU-Parlament deshalb beschlossen, das digitale

Immunsystem der Union durch ein – noch zu gründendes – Kompetenzzentrum für Cybersicherheit sowie ein Netz nationaler Koordinierungsstellen zu stärken.

Zudem wird die Agentur für Netz- und Informationssicherheit (ENISA) zu einer schlagkräftigeren EU-Agentur für Cybersicherheit ausgebaut. Sie soll Mitgliedsstaaten, EU-Institutionen und Unternehmen helfen, sich gegen Angriffe zu wehren. Mit ihrem Cybersecurity Act von 2018 will die EU außerdem einheitliche IT-Sicherheitsstandards für internetfähige Produkte wie Router, aber auch Kühlschränke oder Industriemaschinen flächendeckend einführen.

Cyberangriffe kennen keine Grenzen, Regulierungen und Strafverfolgung schon. Deshalb ist es besonders wichtig für die EU-Mitglieder, ihre Kompetenzen zu bündeln und sich im Kampf gegen Hacker zu vereinen. Dazu gehört auch, Informationen über erfolgte Angriffe auszutauschen. Da die meisten Unternehmen oder Institutionen jedoch Angst vor Imageschäden haben, schweigen sie lieber.

Kernaussagen in Kürze:

- Cyberangriffe können dramatische Auswirkungen auf Wirtschaft und Gesellschaft haben. Besonders anfällig ist die EU mit ihren eng vernetzten Mitgliedsstaaten.
- In acht von zehn europäischen Unternehmen kommt es jedes Jahr mindestens zu einem Vorfall, der die Cybersicherheit betrifft.
- Die EU will sich durch ein – noch zu gründendes – Kompetenzzentrum für Cybersicherheit sowie ein Netz nationaler Koordinierungsstellen künftig besser vor Angriffen schützen.