**Informationssicherheit**

# Umgang mit Cybercrime

Wirtschaftsunternehmen stehen weiterhin weltweit im Fokus von Cyberkriminellen. Deren Ziel ist es, Daten, Knowhow und Informationen auszuspähen bzw. zu stehlen oder die Unternehmen zu erpressen, indem sie mit „Distributed Denial of Service"– sinngemäß Serverüberlastung – drohen. Daneben stellen auch unspezifische, breit gestreute Angriffe (Ransomware) eine hohe Gefahr für die IT-Infrastruktur dar.

Cybercrime umfasst alle illegalen Aktivitäten, die über einen Computer oder ein ähnliches internetfähiges Gerät ausgeführt werden. Angriffsziele sind hierbei meistens Unternehmen. Mittelbar findet hierdurch jedoch auch ein Angriff auf Verbraucher, beispielsweise durch Datenklau, statt.

Die Absichten sind immer gleich: Schaden verursachen und Geld verdienen, z. B. durch einen Zugriff auf Finanzkonten, indem unter fremden Namen Dienstleistungen in Anspruch genommen werden, Dateien gesperrt oder persönliche Daten für Erpressungen abgegriffen werden.

### Kritische Bedrohungslage durch Log4j

Einer der bedeutendsten Cybervorfälle, die in jüngster Zeit bekannt wurden, betraf Apaches Log4j. Die in der Java-Bibliothek entdeckte Schwachstelle führte Mitte Dezember 2021 zu einer kritischen Bedrohungslage.

Log4j ist eine Software, die als Logging Framework verwendet wird, d. h, sie ermöglicht Entwicklern die Überwachung bzw. Protokollierung digitaler Ereignisse auf einem Server. Auf der ganzen Welt wird diese Bibliothek aufgrund ihrer Funktionalität von Programmierern und Systemadministratoren in Rechenzentren in ihre Unternehmensservern, Netzwerkkomponenten und Systemkomponenten eingebunden. Durch die Protokolle lässt sich überprüfen, ob der Betrieb regulär abläuft oder es Anzeichen für ein abnormales Verhalten gibt.

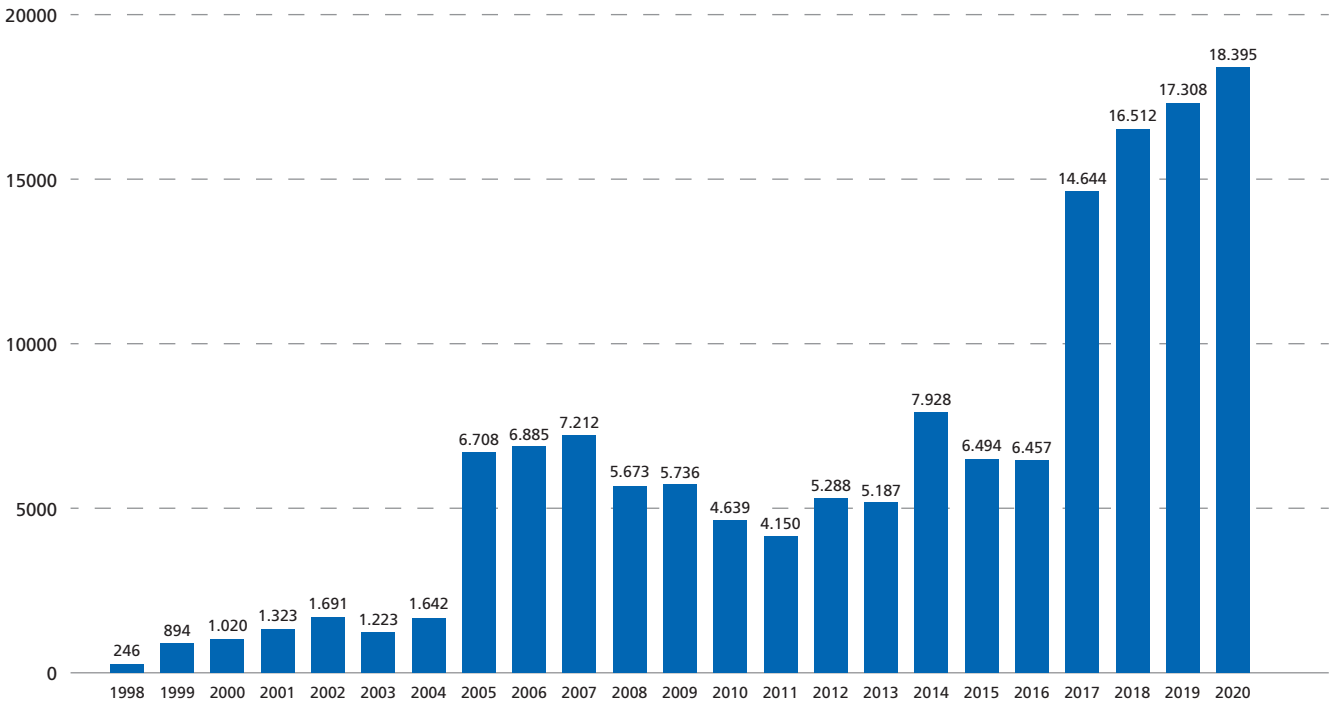
Im aktuellen Fall gestattete ein Fehler nicht autorisierten Benutzern einen ersten Zugang, mit dem sie auf sensible Daten zugreifen und sogar die Servereinstellungen manipulieren konnten. Dies führte zur potenziellen Verwundbarkeit von mehreren Milliarden Computern. Das bedeutete auch, dass Produkte zahlreicher Internetkonzerne schwerwiegende Sicherheitslücken aufwiesen und zeitweise als unsicher galten.

Zwar wurden Updates zwischenzeitlich bereitgestellt. Doch haben nicht alle Dienstebetreiber und Softwareentwickler die nötigen Aktualisierungen vorgenommen, sodass die entsprechenden Systeme weiterhin verwundbar sein können. Zusätzlich zum Update verlangt die gegenwärtige Lage, dass die Systeme und Server nach dem Update auf Unregelmäßigkeiten geprüft werden.

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) rechnen Expertinnen und Experten mit langfristigen negativen Folgen für Unternehmen jeder Größe. Kriminelle könnten die Zeit genutzt haben, um Backdoors und Brückenköpfe zu installieren. Bleiben diese unentdeckt, können sie genutzt werden, um das System/die Daten im Nachgang z. B. auszuspähen, zu manipulieren und/oder zu verschlüsseln. Besteht der Verdacht, dass z. B. Schadsoftware eingeschleust wurde, sollten Betroffene auf bestehende Sicherungskopien zurückgreifen.

Durch die bereitgestellten Updates hat das BSI die Warnstufe von Rot auf Orange herabgesetzt. Das bedeutet jedoch nicht automatisch eine Entwarnung für das einzelne Unternehmen. So banal es klingt: Die Unternehmen müssen sich des Risikos weiter bewusst sein und entsprechend handeln. >

ABB. 1 ANZAHL SCHWACHSTELLEN IN COMPUTERSYSTEMEN NACH KALENDERJAHREN




**Anzahl an veröffentlichten Software-Schwachstellen basierend auf zugewiesenen CVE-Nummern (Common Vulnerabilities and Exposures; Standard zur Benennung von Sicherheitslücken in Computersystemen)**
Quelle der Grafik: Bundeskriminalamt (BKA)

## Patchmanagement – der Weg zu mehr Überblick

Die Anzahl neu entwickelter Schadprogramme wird sich auf hohem Niveau weiterentwickeln. Auch wird sich die Zahl der betroffenen Unternehmen erhöhen. Angriffsszenarien, die regelmäßig bekannt werden, zeigen immer wieder, wie wichtig es ist, die eingesetzte Hard- und Software durch Sicherheits-Updates vor solchen Angriffen zu schützen.

Viele Unternehmen sind jedoch in puncto Updates nicht auf dem neuesten Stand. Trotz der Tatsache, dass Softwarehersteller bemüht sind, fehlerfreie und sichere Programme zu veröffentlichen, sind während des gesamten Produktzyklus Aktualisierungen und Patches erforderlich.

Patches (deutsch Flicken) sind Softwarepakete, mit denen die Hersteller Sicherheitslücken in ihren Programmen schließen. Sie beheben u. a. Programmfehler und verhindern so den Erfolg von Malware-Angriffen (bösartige Software). Ein fehlendes oder vernachlässigtes Patch- und Änderungsmanagement führt daher schnell zu möglichen Angriffspunkten.

In den meisten Unternehmen besteht die IT-Infrastruktur aus einer Mischung älterer wie auch aktueller Technologien. So laufen zum Teil verschiedene Betriebssysteme auf Endpoints und Servern im Netzwerk. Hier werden wiederum Hunderte von geschäftlichen Anwendungen abgebildet, die auf Änderungen im Betriebssystem unterschiedlich reagieren. Sind diese schlecht oder gar nicht gepatcht, bieten sie ein Einfallstor für Angreifer.

Ein zentrales und regelmäßiges Patchmanagement sichert die Einhaltung von Compliance-Regeln und erleichtert die einfache und schnelle Verteilung von Patches.

Um die Ordnung im System zu erhalten, ist es notwendig, eine Übersicht über alle Endpoints im Netzwerk – also Laptops, Desktops, Server und weitere Geräte sowie die darauf installierte Software – zu erstellen. Idealerweise umfasst die Inventarisierung auch die auf den Systemen

AUTORIN UND ANSPRECHPARTNERIN

**Katja Schlüter**
Beauftragte Informationssicherheit und Datenschutz
E-Mail: katja.schlueter@dz-cp.de

installierten Softwareversionen und Softwarelizenzen. Zudem erleichtert eine einheitliche IT-Umgebung die Kontrolle über installierte Softwareprodukte.

Durch ein wirkungsvolles Patchmanagement soll sichergestellt werden, dass Patches zeitnah ausgerollt werden, um Sicherheitslücken erkennen, klassifizieren und beheben zu können:

- Sind Informationen bereitgestellt, sollten die Updates bewertet werden und sollte geprüft werden, ob und wann die Patches installiert werden.
- Speziell bei Clientsoftware ist es empfehlenswert, die Patches vor ihrer Verteilung in einer Testumgebung zu installieren, um möglichen Kompatibilitätsproblemen vorzubeugen.
- Schlussendlich ist das Sammeln von Informationen die Basis für ein angemessenes und wirkungsvolles Patchmanagement. Dabei können Informationen von Drittanbieterquellen, wie entsprechende Informationswebseiten von Herstellern, oder unter www.cert-bund.de abonniert werden.

Ohne ein Patch kann ein Angreifer Sicherheitslücken nutzen, um Serveranwendungen und angeschlossene Geräte fremdzusteuern und Unternehmensnetzwerke zu infiltrieren.

All das Vorgesagte gilt natürlich auch für Computersysteme, die von Privatpersonen genutzt werden.

Im Falle einer Rechnerinfizierung bleibt den Betroffenen nur noch die – hoffentlich funktionierende – Recovery (Wiederherstellungsprozedur) und der Rückgriff auf eine – hoffentlich umfassende – Datensicherung, um an einem Restart-Point vor der Infizierung aufsetzen zu können.

## Fazit

Wer der regelmäßigen Durchführung von Patch-Updates zu wenig Bedeutung beimisst, geht ein unkalkulierbares und hohes Risiko für sein Unternehmen ein. Tagtäglich arbeiten Hacker und Cyberkriminelle daran, Sicherheitslücken in viel genutzten Anwendungen zu finden und für ihre Zwecke zu missbrauchen.

Die Methoden der Cyberangriffe entwickeln sich laufend weiter. Die Konzeption und Implementierung von Schutzmöglichkeiten dagegen können dieser Entwicklung nur mit einer entsprechenden Verzögerung folgen. Um ein jederzeit ausreichendes Schutzniveau aufrechtzuerhalten, muss die Risikoabschätzung zyklisch wiederholt und die IT-Sicherheitslösung ggf. angepasst werden.

IT-Sicherheit stellt somit keinen statischen Zustand dar, sondern muss als ein ständiger Regelkreislauf bzw. andauernder Prozess verstanden werden. ▬