CYBER WAR & IT-SICHERHEIT

Die ohnehin seit Jahren deutlich zunehmende Gefahrenlage im Cyberraum hat mit dem Angriffskrieg Russlands auf die Ukraine nochmals an Schärfe gewonnen. IT-Sicherheit bedarf spätestens jetzt der vollen Aufmerksamkeit und größtmöglichen Wachsamkeit aller Unternehmen, staatlichen Stellen und Organisationen wie der Verbände und verbandsähnlichen Einrichtungen.

Thomas Klauß

WIE REAL IST DIE GEFAHR?

Die IT-Sicherheitswirtschaft und das BSI[1] konnten bereits eine neue schädliche und von langer Hand geplante Malware namens „Hermetic Wiper“ identifizieren – eine Schadsoftware, die Daten bei betroffenen Systemen vollständig und unwiderruflich löschen kann. „Wiper“ wurde zunächst in der Ukraine beobachtet, es wird jedoch auch schon (unbestätigt) über Fälle in anderen Ländern berichtet.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) meldet am 15. März: „Die im Zuge des aktuellen kriegerischen Konflikts von russischer Seite ausgesprochenen Drohungen gegen die EU, die Nato und die Bundesrepublik Deutschland sind mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs verbunden.“[8] Russische IT-Unternehmen, wie auch der Anbieter von IT-Sicherheitslösungen Kaspersky, könnten unter Umständen instrumentalisiert werden.

Schon lange vor dem Einmarsch in die Ukraine hat Russland eine digitale Offensive mit Angriffen im Cyberraum auf militärische und weitere Zielsysteme in der Ukraine gestartet.

Schwere Cyberattacken auf Deutschland und auf die Ukraine haben laut einer aktuellen Untersuchung des Instituts der deutschen Wirtschaft Köln (IW) bereits seit längerer Zeit (auch vor dem Einmarsch in die Ukraine) ihren Ursprung zu einem großen Teil in Russland: Russische Akteure machen mit 28 Prozent der Cybervorfälle die Mehrheit der Fälle mit bekanntem Ursprung hierzulande aus. Die meisten Angriffe auf Deutschland konnten keinem Ursprungsland zugeordnet werden, weil die deutsche Gesetzgebung eine Nachverfolgung erschwert. In der Ukraine konnten dagegen aufgrund der dortigen Rechtslage ungleich mehr Cyberattacken einem Staat zugeordnet werden: Bei vier von fünf Cyberangriffen auf die Ukraine konnte Russland als Herkunftsland bestimmt werden.

Anteil bedeutender Cyberangriffe auf Deutschland und die Ukraine nach Herkunft[2]

Nach der diesjährigen IT-Sicherheitsumfrage von eco, dem Verband der Internetwirtschaft e. V., die vor der Invasion durchgeführt wurde, berichteten auch vor dem Krieg 93,8 Prozent der IT-Sicherheitsexperten von einer wachsenden Bedrohungslage in Deutschland[3].

Insbesondere deutsche Unternehmen sind wirtschaftlich interessante Ziele von Cyberangriffen.

Laut weltweit durchgeführter Umfrage (Quelle Statista[2]) betrugen die Kosten/Verluste durch Cyberattacken im Jahr 2021 in Deutschland durchschnittlich 21.818 Euro je Vorfall gegenüber einem weltweiten Durchschnitt von etwa 11.944 Euro je Vorfall.

Insgesamt wurden die Schäden für die deutsche Wirtschaft durch den Diebstahl von Daten, Spionage und Sabotage für das Jahr 2020 auf 223,5 Milliarden Euro geschätzt. Laut bitkom war der Schaden durch Cyberkriminalität in deutschen Unternehmen 2020 bereits annähernd doppelt so hoch wie 2019.

AUCH DIE PANDEMIE HAT DIE SICHERHEITSLAGE VERSCHÄRFT

Die o. a. Sicherheitsumfrage ermittelte ferner, dass 80 Prozent der IT-Sicherheitsexperten von einer Verschärfung der Gefährdungslage bereits durch die Coronapandemie berichten. Vor allem der durch die Coronakrise ausgelöste Digitalisierungsschub stellt die IT-Sicherheit vor große Herausforderungen.

Insbesondere Homeoffice erhöht das Risiko: So berichten 59 Prozent von 817 in einer bitkom-Studie befragten Unternehmen von Sicherheitsvorfällen, die auf Homeoffice zurückzuführen seien[4].

Heimnetzwerke sind meist wesentlich schlechter geschützt als Firmennetzwerke. In privaten WLANs tummeln sich viele ungesicherte Geräte, wie private Smartphones, Smart Speaker, Sound Bars, Smart-TVs, smarte Küchengeräte, Kameras oder andere Smart-Home-Geräte, die leichter zugängliche Einfallstore für Computer-Viren und andere Bedrohungen sein können als die (hoffentlich) weitaus besser geschützten Firmen-Geräte.

„In Anbetracht der wachsenden Bedrohungslage und Verwundbarkeiten durch mehr Mitarbeiter im Homeoffice schützen sich viele Unternehmen nicht ausreichend vor Cyberangriffen“, sagt Oliver Dehning, Leiter der Kompetenzgruppe Sicherheit im eco – Verband der Internetwirtschaft e. V.

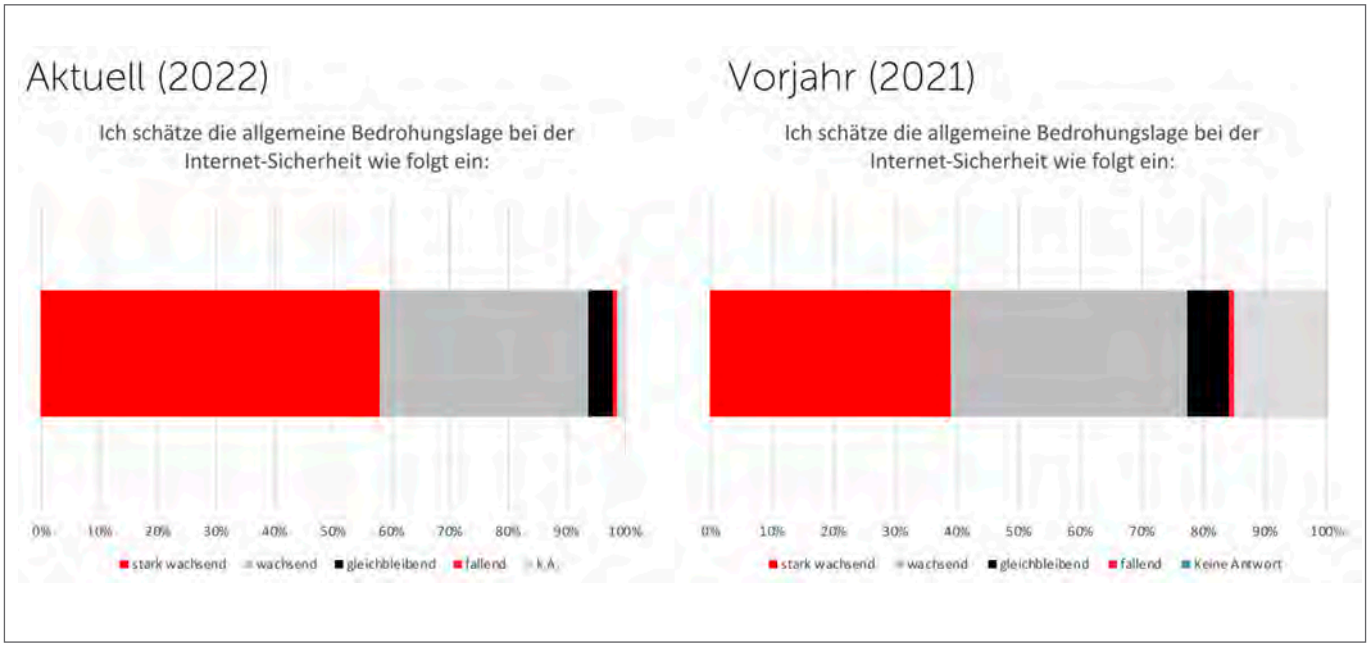
Insbesondere vielen kleinen und mittelständischen Unternehmen fehlt ein Sicherheitskonzept für Remote-Arbeitsplätze. Dazu gehören auch Maßnahmen zur Mitarbeitersensibilisierung.

DIE GRÖSSTEN BEDROHUNGEN, LÜCKEN UND WICHTIGE SICHERHEITSMASSNAHMEN

Wenn es zum IT-Sicherheitsvorfall kommt, dann meistens über eine Ransomware-Attacke (21 Prozent), so die Umfrage des Verbandes[3].

Bei diesen Cyberattacken verschaffen sich Hacker Zugang zum Firmennetzwerk, über das sie auf wichtige Datenbanken, etwa mit allen Buchungs-, Kon-

In den letzten zwölf Monaten berichten 32 Prozent der Unternehmen von Schäden durch IT-Sicherheitsvorfälle[3]



takt-/Kunden-, Produktions- und anderen sensiblen Firmendaten, zugreifen, diese für das Opfer unzugänglich verschlüsseln und anschließend die Zahlung einer hohen Summe (meist in nicht nachverfolgbarer Kryptowährung, wie bspw. Monero) fordern, um die Daten wieder zu entschlüsseln. Dagegen schützt ein fortlaufendes Monitoring der Systeme, mit dem auffällige Zugriffe erkannt werden können.

Auf Platz zwei liegt mit 18 Prozent das Hacking von Websites gleichauf mit dem Diebstahl von Daten.

Übrigens hat nur bei 9 Prozent aller durch Cyberkriminalität Geschädigten eine Versicherung den Schaden aufgefangen.

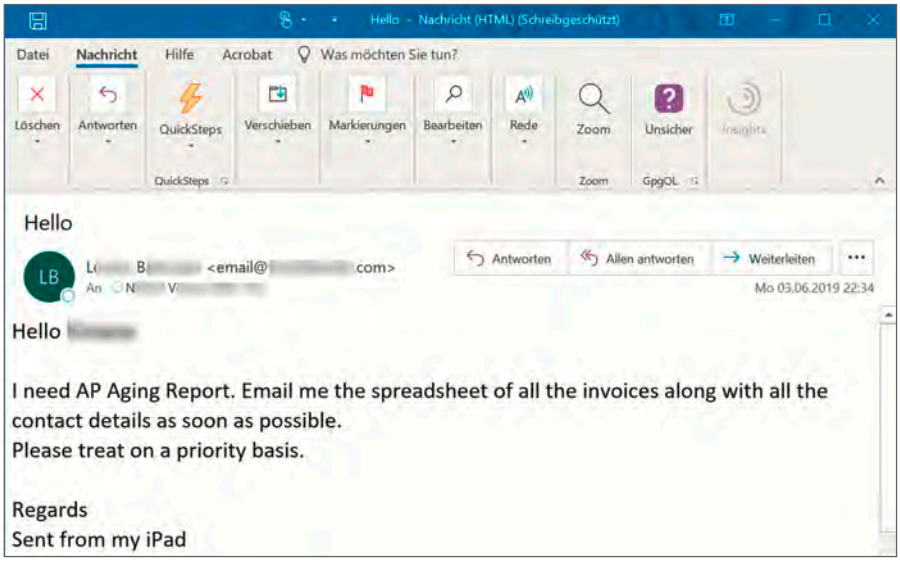
Insgesamt beginnen über 90 Prozent aller Angriffe mit Phishing. Das steht für E-Mails oder Posts, die dazu auffordern, auf einer verlinkten Website Zugangsdaten, Kontodaten o. Ä. einzugeben: Speziell dafür eingerichtete „Fake"-Websites, die so gestaltet sind, dass sie wie Portale seriöser Firmen oder Banken aussehen sollen, fischen die Daten, um sie für eigene, betrügerische Zugriffe einzusetzen.

Solche Attacken können technisch verhindert werden, indem nicht bekannte oder verdächtige E-Mails mit angehängten Dateien in Formaten, die potenzielle Träger von Schadsoftware sein können, automatisch ausgefiltert und in einer „Sandbox" gesichert werden.

Die meisten Organisationen wie auch Verbände haben einfach zu erkennende E-Mail-Adressen nach dem Schema vorname.nachname@verband.de/.org / .net und publizieren diese auch auf ihren Websites oder in LinkedIn, Twitter, Xing etc. Hacker versuchen, sich mit diesen E-Mail-Adressen als Nutzernamen und automatischen Passwort-Tools in Firmensysteme einzuhacken.

Dagegen helfen starke, häufiger geänderte oder maschinell sicher generierte Passwörter, spezielle, nicht einfach recherchierbare Nutzerkennungen und vor allem eine Zwei-Faktor-Authentifizierung über unterschiedliche Geräte (bspw. Laptop plus Smartphone, nicht beides über dasselbe Gerät).

Auch Business-E-Mail-Compromise-Attacken (BEC), sogenannte CEO-Frauds, machen sich einfach zu recherchierende E-Mail-Adressen zunutze: Dabei geben sich die Angreifer etwa als Chef aus und verlangen bspw. eine kurzfristige Überweisung auf ein spezielles Konto oder eine Tabelle mit allen Rechnungen inklusive Kontaktdaten, wie in dem folgenden Beispiel:



Beispiel für einen CEO-Fraud[5]

Solche Manipulationsversuche, die Mitarbeiter und Mitarbeiterinnen dazu bewegen sollen, Links anzuklicken, um Schadsoftware herunterzuladen, Zugangsdaten preiszugeben oder auf Anforderungen in gefälschten E-Mails zu reagieren, fallen unter den Begriff „Social Engineering".

Dementsprechend kann man diesen Bedrohungen am besten mit soziotechnischen, also technisch-organisatorisch-personellen Maßnahmen begegnen – rein technische Lösungen genügen hier nicht.

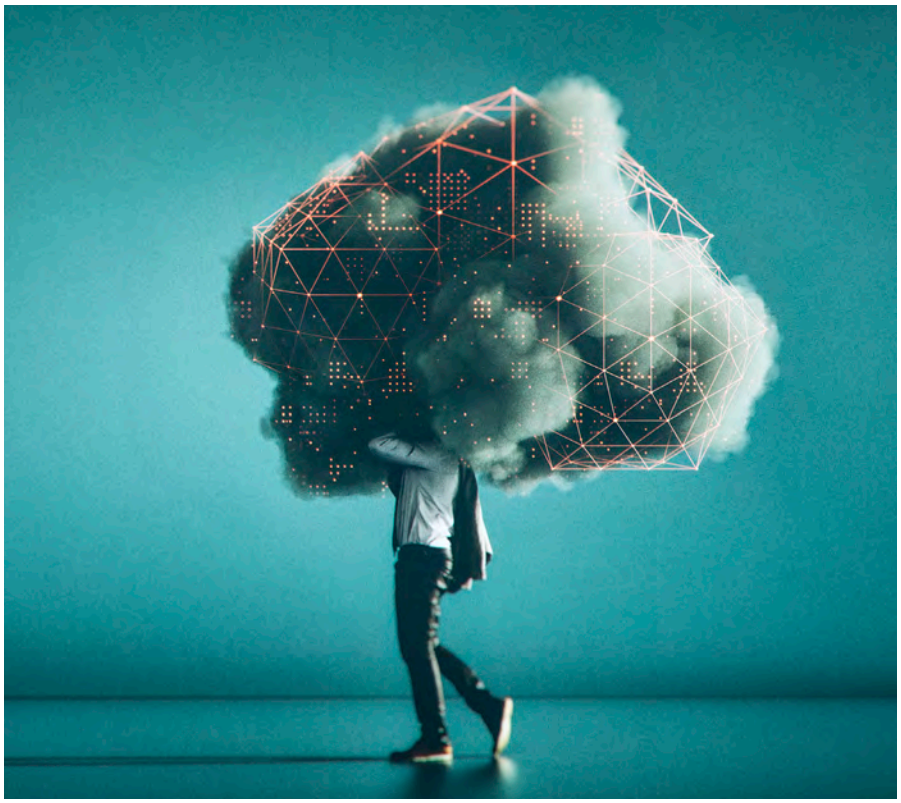
So ist die Sensibilisierung von Mitarbeitern und Mitarbeiterinnen eines der wichtigsten Sicherheitsthemen in den Organisationen – insbesondere im Zeichen von Mobile und Homeoffice!

Sie ergänzt die ohnehin notwendige Notfallplanung, den Schutz vor Schadsoftware und Eindringlingen sowie den Schutz vor gefährlichen und unerwünschten E-Mails.

CHECKLISTE ZU SICHERHEITSMASSNAHMEN

Im Idealfall hätte jede Organisation ein professionelles IT-Sicherheitsmanagement-System nach ISO 27001. Da das mit erheblichen finanziellen, organisatorischen und personellen Aufwänden verbunden ist, besitzen das aber die wenigsten: So enthält die ISO-Norm über 14 Kapitel hinweg eine umfangreiche Auflistung von 35 Maßnahmenzielen (Controls) mit 114 konkreten Maßnahmen zu verschiedensten Sicherheitsaspekten[6].

Selbst mit dem für kleinere oder ressourcenschwächere Organisationen eingeführten BSI-Grundschutz[7] fühlen sich viele überfordert.



Eine Pflichtaufgabe ist jedoch, wenigstens grundlegende technische und organisatorische (Sicherheits-)Maßnahmen (kurz TOM), die ein dem Risiko angemessenes Schutzniveau gewährleisten, zu treffen. Dies ist auch gemäß Datenschutzgrundverordnung, DSGVO Artikel 32, gefordert!

Abschließend noch einmal zusammengefasst wichtige Sicherheitsmaßnahmen:

- Sie benötigen einen Beauftragten für die IT-Sicherheit (nicht selten in Personalunion mit dem Datenschutzbeauftragten).
- Ein solides Zugangs- und Rechtemanagement für Systeme und Räume, in denen Geräte und Server stehen, ist Pflicht.
- Verwenden Sie spezielle Nutzernamen/-Kennungen, starke Passwörter und eine Mehr-Faktor-Authentifizierung.
- Sie müssen alle relevanten Systeme fortlaufend monitoren.
- Geeignete Backup-Strategien helfen, die Arbeitsfähigkeit schnell wiederherzustellen und den Schaden möglichst gering zu halten.
- Ein schärferer Spamschutz und sogenannte Sandbox-Lösungen, die als schadhaft erkannte E-Mails sicher ausfiltern, sollten ebenfalls zur Pflichtübung gehören.
- Sie sollten alle Systeme härten, gegen Zugriff schützen (u. a. über Intrusion Prevention/Detection, IP-Filter ...) und müssen die Software immer auf dem neusten Stand halten.
- Sie müssen organisatorische Maßnahmen treffen und Leitfäden/Regelungen für Mitarbeiter/-innen aufstellen.
- Sie sollten Mitarbeitende sensibilisieren, vor allem bezüglich Homeoffice.
- Sie sollten IT-Administratoren bestmöglich unterstützen.
- Sie sollten Notfallpläne aktualisieren, diese durchspielen und alle aktuellen Hinweise der deutschen Sicherheitsbehörden eng verfolgen. ■

QUELLEN:

[1] www.datenschutz-notizen.de/wp-content/uploads/2022/02/220224_BSI_Empfehlungen_Ukraine.pdf

[2] https://de.statista.com/infografik/26939anteil-der-bedeutenden-cyberangriffe-auf-deutschland-und-die-ukraine-nach-herkunft/?utm_source=Statista+Newsletters&utm_campaign=6a17a5a06e-All_InfographTicker_daily_DE_PM_KW9_2022_Mo&utm_medium=email&utm_term=0_662f7ed75e-6a17a5a06e-314541945

[3] Aus www.eco.de/presse/eco-it-sicherheitsumfrage-2022-unternehmen-reagieren-auf-angespannte-cybersicherheitslage/

[4] www.bitkom.org/Presse/Presseinformation/Lagebericht-IT-Sicherheit-2021

[5] www.heise.de/ct/artikel/Die-Chef-Masche-Wie-CEO-Betrüger-Mails-in-Deutschland-abkassieren-4471915.html

[6] ISO 27001, s. www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/iso-27001?gclid=Cj0KCQiA95aRBhCsARIsAC2xvfzA9-tXp2Nzw6mzCp0TkZDyeMcPrF9INy8_27yRjnLG-qMeOAyIq520aAooFEALw_wcB

[7] BSI-Grundschutz, s. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=1

[8] www.it-business.de/bsi-warnt-vor-verwendung-von-kaspersky-virenschutz-a-1102925/

AUTOR

THOMAS KLAUSS

ist Diplom-Informatiker und Diplom-Medienberater mit mehr als 25 Jahren Erfahrung in der Beratung, Konzeption und Entwicklung sowie im Projekt- und Changemanagement von Digitalisierungsprojekten. Von 2005 bis 2010 war er beim bitkom für die digitale Modernisierung aktiv. Er veröffentlichte außerdem verschiedene Sach- und Fachbücher sowie zahlreiche Artikel.
Seit Ende 2010 berät und unterstützt er Verbände unter X.0 # Verbände digital bei der digitalen Modernisierung (#verbaendedigital) – von Digitalisierungsstrategien über die Maßnahmen-/Projektentwicklung und -Begleitung/Umsetzung bis zum Changemanagement und ist zudem als externer Datenschutz- & Datensicherheitsexperte aktiv.
→ t.klauss@verbaende-digital.de
→ www.verbaende-digital.de