UIMCommunic@tion
praxisnah.gut.informiert.

03/2022
Ausgabe für Österreich

Inhaltsverzeichnis ++ Sicherheitswarnungen des Bundesamts für Verfassungsschutz und für Sicherheit in der Informationstechnik ++ Dringende Empfehlungen der UIMC ++ Neue Webinar-Angebote ++ **Inhaltsverzeichnis**

Die UIMC steht für Frieden, Respekt und Gleichheit und stellt sich klar gegen Krieg, Unterdrückung, Terror und jegliche Form von Gewalt.. im Übrigen nicht nur in der Ukraine, sondern auch in Syrien, Mali oder in Wuppertal. Dies gilt in jeder Gesellschaft und immer, wenn Menschen zusammenkommen.

Die nachfolgenden Aussagen stammen zwar von deutschen Behörden, gelten gleichermaßen auch für Österreich.

Geänderte Bedrohungslage durch Ukraine-Krieg

Bundesämter sprechen explizite Warnungen und Empfehlungen aus

Bundesamt für Sicherheit in der Informationstechnik (BSI)

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html

„Das BSI warnt nach §7 BSI-Gesetz vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky. Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen. […]“

Bundesamt für Verfassungsschutz (BfV)

https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2022-03-04-Sicherheitshinweis.html

„Im Zuge des Krieges in der Ukraine ist neben den militärischen Auseinandersetzungen auf ukrainischem Staatsgebiet auch im Cyberraum eine zunehmende Eskalation zu verzeichnen. Es besteht ein erhöhtes Risiko von Cyberangriffen gegen deutsche Stellen – insbesondere in Reaktion auf die jüngsten Sanktionen und militärischen Unterstützungszusagen. […]

Die steigende Zahl an Cybergruppierungen und sogenannte Hacktivisten, die sich auf beiden Seiten des Konflikts positionieren, erhöht die Anzahl der beteiligten und fähigen Akteure im Cyberraum deutlich, wodurch die Wahrscheinlichkeit für Kollateralschäden erhöht wird. […]“

Empfehlungen des BfV:

„Da die sog. Wiper-Malware nur kurze Zeit benötigt, um ein System zu zerstören, ist Prävention besonders wichtig:

- *Weil der Angreifer für das Platzieren und die Ausführung der Malware eine Zugriffsmöglichkeit auf das System besitzen muss, ist es dringend empfehlenswert, mögliche Angriffsvektoren zu minimieren. **Es ist sorgfältig zu überlegen,** welche Vorgänge und Systeme aktuell für die Gewährleistung der Funktionalitäten eines Unternehmens unbedingt erforderlich sind.*
- ***Backups** müssen in regelmäßigen Abständen angefertigt und anschließend von den betroffenen Systemen getrennt aufbewahrt werden.*
- *Bekannte **Sicherheitslücken** müssen durch das Einspielen vorhandener Update-Patches geschlossen werden und sind somit als Angriffsvektor verschlossen.*
- *Unbekannte oder nicht mehr verwendete Nutzer müssen entfernt und **Berechtigungen** für Nutzer auf ein Minimum reduziert werden.*

Fortsetzung auf der Folgeseite >>

Sensibilisierung der Mitarbeiter auf Gefahren und Bedrohungen

Innerhalb unseres Kurses „Informationssicherheit“ werden die User nicht nur auf erforderliche Maßnahmen geschult, die zum Schutz von Systemen und Informationen zu ergreifen sind, sondern werden anhand von vielen Beispielen auf die Gefahren und Bedrohungen in diesem Zusammenhang sensibilisiert. Somit wird eine große Sicherheitslücke innerhalb von Unternehmen reduziert: Der Mensch bzw. dessen Verhalten beim Umgang mit der IT im Unternehmens-Alltag.

Sie haben noch keinen Zugang? Dann informieren Sie sich unter https://www.uimc.de/ecollege.

UIMC.austria (eine Marke der UIMC Dr. Vossbein GmbH & Co KG), Fleischmarkt 1/6/12, A-1010 Wien
Tel.: +43 1 20 5107 3383, E-Mail: consultants@uimc.at, Internet: www.UIMC.at

» ***Intrusion Detection Management Systeme*** *(IDMS) sollten in der Lage sein, die Malware zu erkennen und zu blockieren. Dafür muss aber dem IDMS die Berechtigung gegeben werden, das Starten und Ausführen entsprechender Prozesse nicht nur zu protokollieren, sondern diese auch sofort zu stoppen und Dateien in Quarantäne verschieben zu können.*

» *Zum Schutz vor (Credential-)Phishing-Angriffen müssen Konten nach Möglichkeit mit Multi-Faktor-* ***Authentifizierung*** *geschützt werden.*

» ***Misstrauen Sie allen E-Mails****, die Sie zu dringenden Handlungen auffordern. Geben Sie niemals Ihre Passwörter an und klicken Sie niemals auf Links oder Anhänge verdächtiger E-Mails. Dies gilt auch für E-Mails von Familie, Freunden oder dem Arbeitgeber. Deren E-Mail-Konten könnten ebenfalls gehackt worden sein.*

» *Die aktuelle Bedrohungslage muss den Mitarbeiterinnen und Mitarbeitern bekannt gemacht werden, um ein* ***Gefährdungsbewusstsein*** *zu schaffen.*

» *Etablierung und Bekanntmachung von* ***Meldeprozessen*** *bei Auffälligkeiten und Sicherheitsvorfällen innerhalb des Unternehmens. [...]“*

Empfehlungen der UIMC zur Verbesserung der Sicherheit

1. **Prüfen Sie Ihre Systeme** insbesondere im Hinblick auf bekannte Sicherheitslücken und Erforderlichkeit von User-Rechten.
2. Hinterfragen Sie die Nutzung von Kaspersky-**Virenschutzsoftware**.
3. **Schärfen Sie das Bewusstsein** Ihrer Mitarbeiter; hierzu eignen sich einerseits Rundschreiben mit Hinweisen und andererseits Schulungsmaßnahmen, wie beispielsweise unser eCollege-Kurs „Informationssicherheit“.
4. Schaffen Sie **Meldeprozesse** für etwaige Sicherheitslücken und Vorfälle.
5. Beginnen Sie mit dem Aufbau eines zielgerichteten Informationssicherheits-Managementsystems (**ISMS**), indem Sie die aktuelle Sicherheits- und Risikosituation überprüfen.
6. **Prüfen Sie die o. g. Empfehlungen des BfV** unter Berücksichtigung der allgemeinen und individuellen Risikosituation; halten Sie ggf. Rücksprache mit unseren Experten für Informationssicherheit.

Sie haben das letzte web.eCollege verpasst, würden aber gerne noch mehr zum Thema „8 praktische Kniffe bei der Revision im Datenschutz “ erfahren? Dann schauen Sie sich die Unterlagen und/oder die Aufzeichnung an:
http://update.uimcollege.de

Sie können sich als Gast anmelden. Hierzu geben Sie bitte den Code ein, den Sie bei uns erfragen können.
Sofern Sie als Kunde bereits Zugangsdaten für einen anderen Kurs im eCollege haben, können Sie sich auch „selbst einschreiben“. Die Einschreibung bleibt einen Monat bestehen.

web.eCollege
kompakt praxisnah informieren

Die nächsten Termine [kostenfrei]

13.04.2022: 5 Anforderungen beim Drittlandtransfer

11.05.2022: 7 wichtige Aspekte bei der Risikobewertung

13.07.2022: 7 nützliche Tipps für eine Lieferantenbewertung / Dienstleister-Auditierung

Anmeldung unter www.uimc.at/webecollege

Aktuelles im Online-Formular-Center

» keine wesentlichen Updates oder Neuerungen im März

Um über Neuerungen zeitnah informiert zu werden, können Sie künftig unser News-Forum abonnieren und erhalten daraufhin eine E-Mail (siehe oben).

www.online-formular-center.eu