SICHERHEIT IN KRISEZEITEN

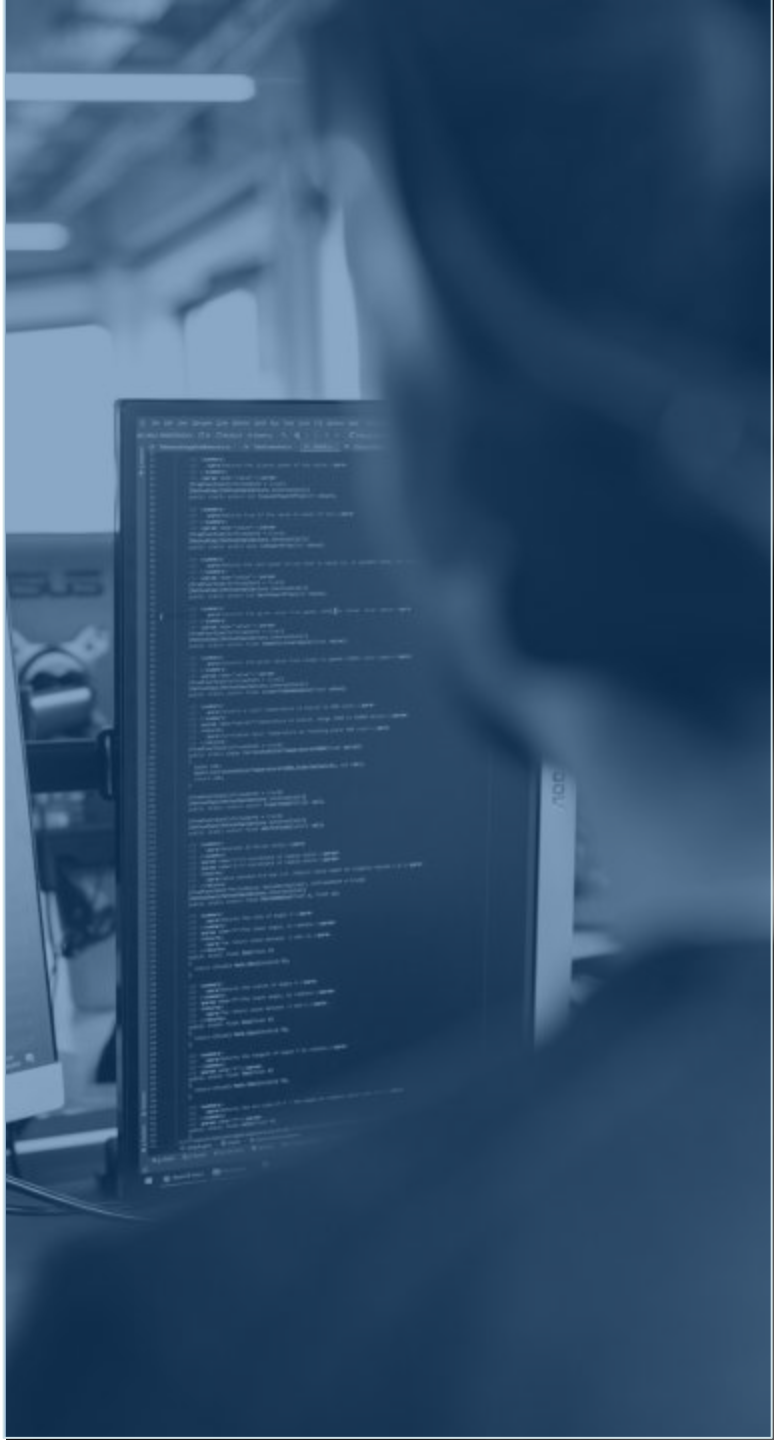
March, 2022

Powered by CYBEREADY

Warum es wichtig ist

Die Cyber-Aktivitäten nehmen rund um den Konflikt zwischen Russland und der Ukraine zu, und obwohl wir vielleicht nicht direkt in den Konflikt verwickelt sind, sind wir dennoch alle davon betroffen.

Jede weltweite Krise entwickelt ihre eigene Cyber-Dimension und die starke Zunahme an bösartigen Phishing-E-Mails zeigt, dass es sich bei dieser Krise nicht anders verhält.



Was vor sich geht

1 Beide Seiten haben Cyberangriffe mit datenlöschender Malware, offline geschalteten Websites usw. gestartet, um eine legitime Nutzung zu verhindern.

2 Diese Angriffe sind nicht immer begrenzt und infizieren oft Geräte und Websites, die nicht am Konflikt beteiligt sind. Dazu gehören auch Ihre geschäftlichen und privaten Geräte.

3 Auch Ihre persönlichen Social-Media-Konten könnten gehackt werden, um falsche Informationen oder Malware zu verbreiten.

Wie Sie Ihr Heimnetzwerk schützen können

Installieren Sie das neueste Betriebssystem und alle Sicherheitsupdates. Sobald diese verfügbar sind, sollten Sie eine Benachrichtigung auf Ihrem Computer oder Smartphone sehen.

Richten Sie für Social-Media-Konten (Facebook, Linkedin, Twitter usw.) und E-Mail-Konten eine Zwei-FaktorAuthentifizierung ein. Richten Sie nach Möglichkeit auch ein Backup-E-Mail-Konto ein.

Informieren Sie Freunde und Familie über diese Vorgänge und fordern diese auf, dasselbe zu tun.

Wie Sie unser Netzwerk schützen können

Weil wir uns um die interne Netzwerksicherheit kümmern, müssen Sie sich um keine technischen Angelegenheiten kümmern.

Während dieser Zeiten könnten Sie vermehrt Phishing-Angriffe erhalten. Nehmen Sie sich vor E-Mails in acht, in denen Sie um technische oder finanzielle Hilfen gebeten werden.

Überprüfen Sie weiterhin die E-Mail-Adresse der Absender – denken Sie daran, dass dies der wichtigste Schritt bei der Erkennung von Phishing-Angriffen ist.