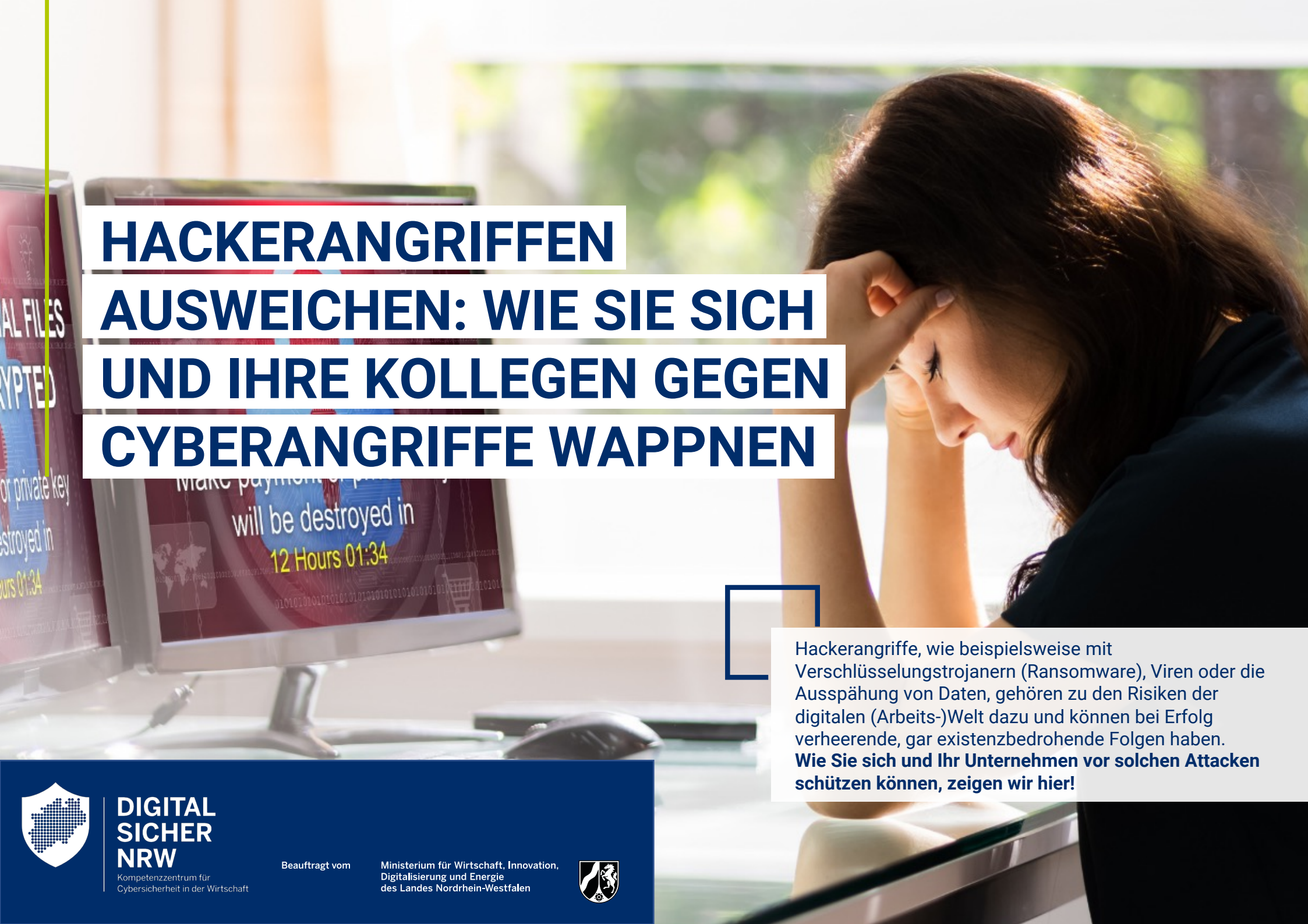
HACKERANGRIFFEN AUSWEICHEN: WIE SIE SICH UND IHRE KOLLEGEN GEGEN CYBERANGRIFFE WAPPNEN



Hackerangriffe, wie beispielsweise mit Verschlüsselungstrojanern (Ransomware), Viren oder die Ausspähung von Daten, gehören zu den Risiken der digitalen (Arbeits-)Welt dazu und können bei Erfolg verheerende, gar existenzbedrohende Folgen haben. **Wie Sie sich und Ihr Unternehmen vor solchen Attacken schützen können, zeigen wir hier!**

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

DIGITAL SICHER NRW

ANTWORTEN AUF DIE WICHTIGSTEN FRAGEN

WAS SIND DIE ANGRIFFSZIELE IM UNTERNEHMEN?

Bei einer digitalen Attacke auf ein Unternehmen haben es die Angreifenden oft auf folgende „Beute“ abgesehen:

- Sensible Daten
- Kundendaten, die im Anschluss weiterverkauft werden können
- Erpressung von bspw. Lösegeld, etwa durch Unkenntlichmachung von Daten, z.B. durch einen Ransomware-Angriff

WIE ERFOLGT EIN HACKING-ANGRIFF AUF EIN UNTERNEHMEN?

Erfolgreich durchgeführte digitale Angriffe sind in vielen Fällen auf unzureichend gesicherte IT-Infrastruktur, unsichere Webserver oder Netzwerke zurückzuführen. Trotzdem ist der Mensch das größte Sicherheitsrisiko für ein Unternehmen. Mindestens zwei Drittel der erfolgreichen Angriffe sind auf „Fehlverhalten“ bzw. Unaufmerksamkeiten unwissender Mitarbeitenden zurückzuführen.

AUF WELCHE ART UND WEISE WERDEN MITARBEITENDE GETÄUSCHT?

Bei vielen Angriffen auf digitale Unternehmensstrukturen werden unwissende Mitarbeitende für die Zwecke der Angreifenden genutzt.
So beispielsweise durch:

- Übernahme von Mailkonten / Identitätsdiebstahl (Social Engineering)
- Gefälschte Portale (Phishing)
- Einschleusen schadhafter Dateien per E-Mail (Phishing)

DIGITAL SICHER NRW

DIE WICHTIGSTEN ABWEHRMAßNAHMEN

UNSICHERE IT / WEBSERVER / NETZWERKE

Um einer unsicheren IT vorzubeugen, sollten Verantwortlichkeiten festgelegt und ein IT-Administrator ernannt werden. Dieser Administrator sollte im Bereich der digitalen Sicherheit geschult sein und einen Überblick über u.a. folgende Punkte haben:

- Aktualität der Betriebssysteme und der genutzten Programme – Update-/ Patchmanagement
- Etablierung und Betrieb von Sicherheitsmechanismen wie Firewall oder Antiviren-Software
- Backupmanagement
- Notfallmanagement

RISIKOFAKTOR MENSCH

Der Faktor Mensch gehört zu den größten Sicherheitsrisiken für ein Unternehmen, weswegen eine umfassende Sensibilisierung für Geschäftsführende und Mitarbeitende gleichermaßen unabdingbar ist. Dazu gehören unter anderem:

- Regelmäßige Awareness-Schulungen für das **gesamte** Personal
- Verantwortlichkeiten festlegen
- Sichere Passwortpolitik mit entsprechenden Regelungen
- Klare Regelungen für den Umgang mit E-Mailanhängen, externen Speichermedien und Updates für das Arbeitsgerät
- Besonders wichtig: Etablierung einer Fehlerkultur. Durch Fehler können wir lernen!

DER SCHUTZ DER IT-STRUKTUR UND DIE SENSIBILISIERUNG VON MITARBEITENDEN ALS SCHUTZ VOR DIGITALEN ANGRIFFEN

Um digitalen Attacken keine Angriffsfläche zu bieten, ist es zum einen wichtig, dass IT-Systeme im Unternehmen mit Hilfe von Updates stets auf dem neusten Stand gehalten werden müssen. Zudem sollten Sie mit Hilfe verschiedener Lösungen abgesichert sein. Zum anderen trägt die Schulung aller Mitarbeitenden zu einer ganzheitlichen Verbesserung der digitalen Sicherheit in der Firma bei.

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen