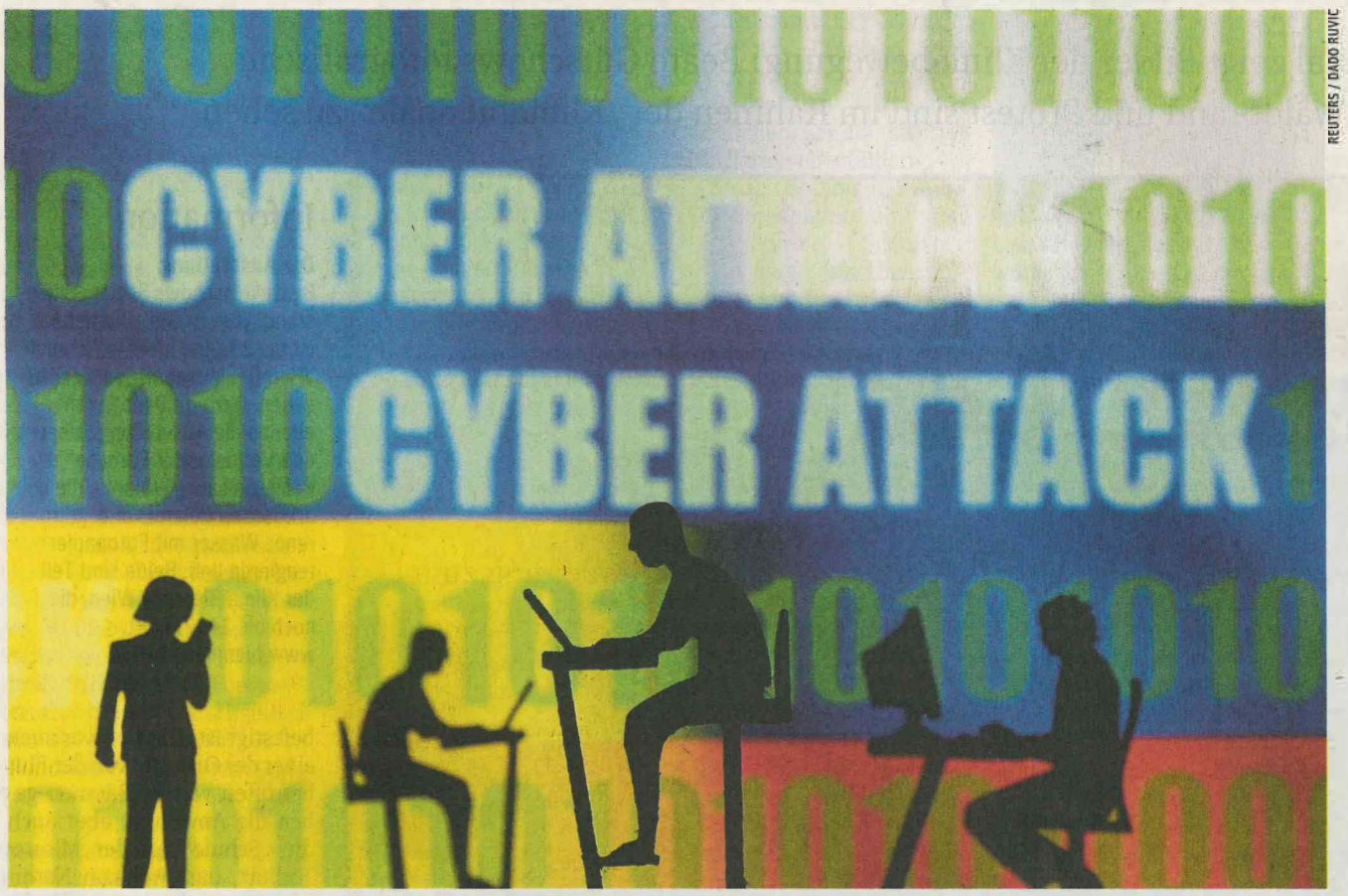
Neue IT-Sicherheitsregeln für Firmen

EU-Richtlinie. Ein neues Gesetz soll die Cybersicherheit erhöhen. Bis zu 6.000 heimische Unternehmen und Behörden müssen Risikoanalysen erstellen und Maßnahmen zum Schutz vor Angriffen ergreifen



REUTERS / DADO RUVIC

Die Richtlinie für Netz- und Informationssicherheit (NIS 2) muss bis Oktober umgesetzt werden

VON **PATRICK DAX**

Mit Cyberangriffen hat fast jedes Unternehmen zu tun gehabt. Nicht wenige davon sind erfolgreich. Die Schäden können enorm sein und von Betriebsunterbrechungen bis zum Datenverlust reichen. Bis Oktober muss in Österreich eine EU-Richtlinie umgesetzt werden, die das Cybersicherheitsniveau erhöhen soll. Was aber bedeutet das NIS 2 genannte Regelwerk für Unternehmen? Der KURIER fasst die wichtigsten Fragen und Antworten zusammen.

? Was soll mit dem Gesetz erreicht werden?

Die Widerstandsfähigkeit gegen Cyberangriffe soll erhöht werden, sagt Marc Nimmerrichter, Geschäftsführer des Beratungsunternehmens Certitude Consulting. Zwar hätten sich viele Unternehmen auch schon bisher gegen Cyber-Vorfälle geschützt, jetzt sei das aber gesetzlich gefordert.

? Welche Unternehmen sind betroffen?

Betroffen sind vor allem große und mittlere Unternehmen mit mehr als 50 Beschäftigten und mehr als 10 Millionen Euro Jahresumsatz der kritischen Infrastruktur. Der Begriff ist weit gefasst und reicht von Energie, Verkehr, Banken, digitaler Infrastruktur bis zu Postdiensten und dem herstellenden Gewerbe. Für kleine Firmen, die im Bereich der digitalen Infrastruktur tätig sind, gelten die Regeln ebenfalls. Auch Behörden müssen sich daran halten. Insgesamt dürften bis zu 6.000 Firmen betroffen sein, schätzt Nimmerrichter.

? Welche Anforderungen müssen sie erfüllen?

Sie müssen sich im Innenministerium registrieren und etwa Risikoanalysen erarbeiten und Maßnahmen zur Minimierung von Vorfällen einleiten. Sie müssen Schulungen durchführen oder Verschlüsselung einsetzen und sind angehalten, die Sicherheit ihrer Lieferanten zu überprüfen.

? Wie viel wird das die Firmen kosten?

Das sei von der Größe des Unternehmens abhängig und davon, wo es bei der Cybersicherheit stehe, sagt Nimmerrichter. Für einen kleinen Maschinenbauer mit 60 Angestellten rechnet der Experte mit Mehrkosten zwischen 5.000 und 50.000 Euro.

? Werden Firmen finanziell unterstützt?

Die Forschungsförderungsgesellschaft FFG unterstützt Firmen mit bis zu 10.000 Euro und bis zu 40 Prozent der Kosten. Der Cyber Security Scheck kann aber nur bis zum 15. April, beantragt werden.

? Müssen Vorfälle gemeldet werden?

Erhebliche Vorfälle müssen unverzüglich, spätestens aber innerhalb von 24 Stunden, nachdem sie bekannt wurden, dem Computer Emergency Response Team (CERT) oder den sektorspezifischen CERTs gemeldet werden.

? Welche Strafen drohen Firmen, die sich nicht an die Regeln halten?

Bis zu 10 Millionen Euro oder bis zu 2 Prozent des Jahresumsatzes. Geschäftsführer haften persönlich, wenn ein Schaden entsteht. „Das wird einen Effekt haben", sagt Nimmerrichter.

? Wann tritt das Gesetz in Kraft?

Derzeit befindet sich das Gesetz in Begutachtung. In Kraft treten wird es voraussichtlich am 18. Oktober. Denn bis dahin muss die EU-Richtlinie, national umgesetzt werden.

Wie sich NIS 2 auf Mitarbeiter auswirkt

Schulungen und Zutrittskontrollen

Interview. Die Anpassung an die NIS-2-Richtlinie wird in Firmen nicht nur IT-Abteilungen beschäftigen, auch andere Angestellte sind betroffen. Der KURIER hat mit Sebastian Klocker, Datenschutzexperte beim Österreichischen Gewerkschaftsbund, gesprochen.

KURIER: Welche konkreten Maßnahmen müssen Unternehmen umsetzen, um NIS-2-konform zu sein?

Sebastian Klocker: Es müssen Risikoanalysen im kompletten Unternehmen durchgeführt werden. Es muss klar festgelegt werden, wer was zu tun hat, wenn es zu einer Cyberattacke oder einer Erpressung mittels Ransomware kommt. Zugriffsberechtigungen sind auch enorm wichtig. Wer hatte wann Zugriff auf Computer, was hat die Person da gemacht?

Welche Änderungen wird es für Mitarbeiter geben?

Beim Personalmanagement kann es für Stellen in sensiblen Bereichen zu Hintergrundchecks kommen. Ein wichtiger Aspekt werden auch Fortbildung und Sensibilisierungsmaßnahmen sein.

Für Vorstand, Aufsichtsrat und Geschäftsführung sind Sicherheitsschulungen Pflicht. Anderen Mitarbeitern müssen Schulungen angeboten werden. Was soll darin vermittelt werden?

Es wird definitiv darum gehen, Wissen zur Erkennung und Bewertung von Cybersicherheitsrisiken zu erlangen. Für jeden Angestellten wird es unterschiedliche Anforderungen geben, je nachdem, in welchem Bereich die Person arbeitet. Im Büroalltag ist Phishing eines der größten Probleme. Mit dem Aufkommen von generativer Künstlicher Intelligenz ist die Gefahr gestiegen. Wichtig wäre, dass Mitarbeiter wissen, wie sie eMails prüfen können. Außerdem muss es eine Meldemöglichkeit geben.

Wie streng müssen Zugangskontrollen gestaltet sein? Reicht eine Chipkarte oder braucht es biometrische Methoden wie einen Fingerabdruck-Scanner?

Jedes Unternehmen muss das anhand seiner Risikoanalysen selbst einschätzen. Es muss immer das gelindeste, am wenigsten invasivste Mittel genommen werden, das nicht in die Privatsphäre der Mitarbeiter eingreift.

Was wäre nicht erlaubt?

Videoüberwachung von jedem Arbeitsplatz etwa. Bei Maßnahmen, die das Potenzial haben, die Menschwürde anzugreifen, ist eine Vereinbarung mit dem Betriebsrat notwendig. Der wird sich nicht querstellen, wenn eine Maßnahme notwendig ist, aber Daten, die dabei anfallen, dürfen wirklich nur zu Zwecken der IT-Sicherheit und nicht zur Leistungskontrolle eingesetzt werden.

DAVID KOTRBA