IHK Schwarzwald Baar Heuberg

Thema des Monats

Daten | Fakten | Argumente

1. Mai 2022

Krieg in der Ukraine bedeutet Handlungsbedarf bei Cybersicherheit

Der Krieg in der Ukraine wird in zunehmendem Maße von Hackerangriffen begleitet. Die zumeist unbekannten Verursacher zielen vor allem auf kritische Infrastrukturen sowie Anbieter von digitalen Netzen und Diensten. Mittlerweile erreichen die Attacken auch den Mittelstand. Betroffen sind etwa Zulieferer und Dienstleister größerer Akteure sowie Nutzer von bislang als vertrauenswürdig geltender IT-Sicherheitssoftware.

IT-Sicherheit in Unternehmen: Luft nach oben

Die Mehrheit der Mittelständler arbeitet auf einem Cybersicherheits-Niveau, das einem gezielten, professionellen und massiven Angriff nur wenig entgegenzusetzen hat. Zwar legen fast alle Unternehmen regelmäßige Sicherungskopien ihrer Datenbestände an und verfügen über Firewalls und Virenschutz. Doch nur 31 Prozent der Unternehmen haben einen klaren Plan dafür, wie in einem Notfall vorzugehen ist.

Betriebe sollen ihren IT-Sicherheitsabstand überprüfen und anpassen

Jede konkrete und netzsichernde Maßnahme ist gut – selbst, wenn sie spät kommt. Mittlere und größere Unternehmen sollten ihre Mitarbeiterinnen und Mitarbeiter daher für die Sicherheitsproblematik sensibilisieren, den Stand ihrer IT-Systeme in Bezug auf Updates, Backups und dergleichen prüfen sowie Sperrlisten (sogenannte Blacklists) zur Abwehr von Internetverkehren aus Russland führen. Auch kleineren Unternehmen ist dringend zu raten, ihre Sicherheitswerkzeuge zu prüfen – also Virus-Scanner, Router, Firewall, Verschlüsselung und Archivierung. Betriebe sollten sicherstellen, dass ihre Tools aktiv und aktuell sind sowie regelmäßig überprüft und gepatcht werden. Im Falle irritierender Phänomene bei der Nutzung von Mail, Webdiensten oder Datenübertragung empfiehlt es sich, den IT-Dienstleister zu Rate zu ziehen.

Versprechen aus dem Koalitionsvertrag zeitnah umsetzen

Die Bundesregierung hat sich viel vorgenommen, um die Daten- und Informationssicherheit in den Unternehmen zu verbessern. Mit verschiedenen Maßnahmen sollen Sicherheitslücken geschlossen und Sicherheitsvorgaben für Produkte beziehungsweise Anwendungen eingeführt werden. Bestenfalls sollten Letztere mit bereits „eingebauter Sicherheit" und ohne Sicherheitslücken hergestellt werden. Die Produkte und Anwendungen sollen zugleich schon mit der Auslieferung an die Nutzer datenschutzkonform vorkonfiguriert sein. Vorgesehen ist auch eine Herstellerhaftung für Schäden, die fahrlässig durch Programmfehler in Produkten verursacht werden. Der Koalitionsvertrag sieht richtigerweise vor, dass der Staat keine IT-Sicherheitslücken aufkaufen oder offenhalten darf, um sie beispielsweise für Überwachungszwecke zu nutzen. Er soll vielmehr darauf hinwirken, dass diese Lücken schnellstmöglich geschlossen werden. Nur dann können Unternehmen im digitalen Raum sicher agieren. Ersatzteile und Software-Updates für IT-Geräte sollen den Plänen zufolge künftig für die übliche Nutzungsdauer verpflichtend verfügbar sein.

Handreichungen zum Vorgehen in der aktuellen Lage

Unter den folgenden Quellen finden Unternehmen weitere Hinweise zum Thema:

- Beim konkreten Einstieg in passgenaue IT-Sicherheitsmaßnahmen im Unternehmen hilft die Transferstelle für IT-Sicherheit im Mittelstand. Sie hat auch fünf Sofortmaßnahmen veröffentlicht.
- Das Bundesamt für Sicherheit in der Informationstechnik hat Maßnahmenempfehlungen im Hinblick auf die aktuelle Lage in der Ukraine zusammengestellt.
- Auch das Bundesamt für Verfassungsschutz hat Sicherheitshinweise herausgegeben. Mehr darüber erfahren Sie hier.
- Unter www.ihk.de finden Sie Informationen zur Daten- und Informationssicherheit der IHK-Organisation, insbesondere das Infoblatt Einstieg ins IT-Notfallmanagement für KMU, eine Notfallkarte zur Information der Mitarbeitenden im Unternehmen sowie einen Leitfaden „vertrauenswürdige IT-Dienstleister".

Fragen zum Thema des Monats?
Christian Beck, IHK-Pressestelle, Telefon: 07721 922-174, E-Mail: beck@vs.ihk.de.