IT-SICHERHEIT – Diebstahl von Daten und unbemerktes Einschleusen von Trojanern: Ist Ihr Unternehmen genügend geschützt?

Mehr digitale Angriffe auf KMU

Seit den Enthüllungen von Edward Snowden sind viele Unternehmen alarmiert, möchte man meinen. Sie fragen sich, ob ihre Firmen-IT sicher ist, die Kundendaten und die Innovationen geschützt sind und was sie überhaupt dagegen unternehmen können, um ihre IT effektiv abzusichern. Die Unsicherheit verstärkt sich noch durch aktuelle Schlagzeilen zu den vielen «Einbrüchen» in Firmennetze nebst Diebstahl von Daten, unbemerktem Einschleusen von Trojanern, Phishing Mails, gratis Outlook für iPad/iPhone, Angriffen auf Industrieanlagen, Einsatz von Spionage-Tools (versteckter GSM-Spion, kleiner Videokamera, Smartphone-Spion) oder gezielten Angriffen auf Manager in den Hotels. Diese realen Bedrohungen werden durch nicht sensibilisierte Mitarbeitende, fehlendes Risikomanagement, Mittel und Ressourcen für die Planung und Umsetzung der Sicherheitsmassnahmen, unzureichende Weisungen, mobile Endgeräte (BYOD), Cloud-Computing, falsche Zugriffsberechtigungen und unsichere Software-Applikationen noch verschärft.

Es reicht längstens nicht, das Passwort regelmässig zu ändern. Vor allem KMU sind häufig von digitalen Attacken betroffen. Diese treffen fast jedes dritte Unternehmen.

KMU am stärksten betroffen

Am stärksten sind KMU von digitalen Attacken betroffen. Diese treffen fast jedes dritte Unternehmen. Vor allem innovative Unternehmen mit ihrem spezialisierten Know-how in bestimmten Märkten und Technologien wecken bei kriminellen Hackern und Geheimdiensten Begehrlichkeiten und führen zu einem oft stark unterschätzten Risiko. Wenn Ihr Auto gestohlen wird, bemerken Sie dies sofort. Wenn Daten geklaut werden, merken Sie es in der Regel nicht oder erst sehr spät (zum Beispiel erst dann, wenn Ihre Mitwerber immer mehr Aufträge erhalten). Der Grossteil der Angriffe findet allerdings vor Ort statt. Dabei handelt es sich häufig um gezielten Datenklau von aktuellen oder ehemaligen Mitarbeitenden oder um das Einschleusen von Schadsoftware infizierten Datenträgern wie beispielsweise USB-Sticks. Hinzu kommen neue Entwicklungen oder Ereignisse in der eigenen Firma, Attacken von Monopolisten und Mitwerbern oder ungeahnte Sicherheitslücken in der Software. Die Herausforderung besteht folglich darin, Ihre Daten und Ihr Know-How mit angemessenen technischen und organisatorischen Sicherheitsmassnahmen auf Basis einer zuverlässigen und möglichst vollständigen Risikoanalyse zu schützen und ein ausgewogenes Gleichgewicht zwischen den Risiken, der Benutzerfreundlichkeit und den Kosten herzustellen.

Wie schützen?

Es lohnt sich, Zeit und Geld zu investieren, um Mitarbeitende für Sicherheitsrisiken zu sensibilisieren und klare Richtlinien aufzustellen. Denn die teuersten Firewalls und Securitylösungen bringen Ihnen nichts, wenn Ihre Mitarbeitenden Ihr Unternehmen durch ein falsches Verhalten, durch die Verwendung von Dropbox, unsichere USB-Sticks oder Phishing-Mails gefährden. Hier einige Tipps zum richtigen Schutz in Ihrem KMU:

- Wählen Sie gute Passwörter mit Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- Wechseln Sie Ihre Passwörter regelmässig (zum Beispiel alle 180 Tage).
- Mitarbeitenden nur diejenigen Zugriffsrechte gewähren, welche sie für die Ausführung ihrer Arbeit benötigen (Need-to-know-Prinzip).
- Ihren Rechner immer mit den aktuellsten Updates schützen und den Virenschutz täglich aktualisieren.
- Scannen Sie Ihr Netzwerk regelmässig auf mögliche Schwachstellen (zwei Mal im Jahr).
- Erstellen Sie Weisungen für alle Mitarbeitenden (beispielsweise Umgang mit Passwörtern, Informationen, E-Mail und Internet).
- Sichern Sie Ihre Unternehmensdaten täglich und bewahren Sie diese auch extern an einem sichern Ort auf.
- Seien Sie vorsichtig mit dem Einsatz von Clouddiensten.
- Sensibilisieren Sie Ihre Mitarbeitenden (Umgang mit USB-Stick, Smartphone oder Phishinggefahr).
- Seien Sie vorsichtig beim Surfen im Internet und verwenden Sie nur Software von sicheren Quellen.
- Achten Sie auf E-Mails in einer anderen Sprache, Rechtschreibefehler, Rabattversprechen, angebliche Lotteriegewinne und unbekannte Absender.
- Schützen Sie Ihr WLAN-Netzwerk mit einem starken Passwort und der WPA2 Verschlüsselung.
- Erarbeiten Sie eine BYOD-Strategie für den Umgang mit Smartphones, Tablets und Notebooks.

Wolfgang Sidler

LINK

www.sidler-security.ch