Was aber, wenn die Stadtmauer fällt?

Man könnte sich ein Unternehmen wie eine mittelalterliche Stadt vorstellen. Die Schatzkammer oder der Bergfried ist das Herzstück des Unternehmens (Kundendaten, Geschäftsgeheimnisse, administrative Benutzer). Rundherum gibt es eine (mehr oder weniger) starke Verteidigung. Ganz außen eine Mauer.

Mit externen IT-Security Assessments hat man die äußere Mauer eigentlich schon ganz gut im Griff - nur wenige Dienste hängen im Internet. Mittlerweile ist auch allgemein bewusst, dass außerhalb unserer Stadtmauern etwas lauert, das rund um die Uhr versucht, Lücken zu finden.

Aber es wäre ein Fehler, sich nur auf die äußeren Mauern der Stadt zu konzentrieren. Das wussten schon die Menschen im Mittelalter - eine zweite oder dritte Stadtmauer und die Existenz des Bergfrieds zeugen davon. Doch in den Unternehmen ist das Bewusstsein für diese “Defense in Depth”, also “Verteidigung in die Tiefe”, oft noch nicht so ausgeprägt vorhanden.

Klar, die Frage, wie weit ein Hacker kommen kann, wenn er erst einmal “drin” ist, will man sich vielleicht gar nicht stellen. Scrollt man durch öffentlich gewordene Ransomware-Opfer (die Dunkelziffer ist natürlich viel höher), wird schnell klar: “Passiert uns nicht” ist keine Strategie. “Wir sind zu klein” ebenfalls.

Bleibt entweder den Kopf in den Sand zu stecken und abzuwarten, bis jemand die Stadtmauern durchbricht. Oder man fragt sich: Was passiert, wenn (und es keine Frage das „ob“) die Stadtmauer fällt?

Ein paar Tipps, wie die Verteidigung innerhalb der Stadtmauer verbessert werden könnte:

#TIPP 1:

Stellen Sie sicher, dass Sie eine gute „Stadtwache“ haben:

EDR-Lösungen (Endpoint Detection and Response) gehen weit über den klassischen Antivirus hinaus. Sie erkennen nicht nur Schadsoftware selbst, sondern auch verdächtiges Verhalten von Nutzer:innen und Rechnern.

#TIPP 2:

Möglichst wenige Personen haben den Schlüssel zur „Schatzkammer“:

Eine zu leichtfertige oder zu breit gestreute Verteilung von Berechtigungen macht es einem Hacker sehr leicht, die Schatzkammer vielleicht sogar direkt zu leeren. Wenn Sie „Active Directory“ verwenden, können Sie z.B. in Zusammenarbeit mit Ihrem IT-(Sicherheits-)Dienstleister eine Active Directory-Analyse hinsichtlich Berechtigungen und Fehlkonfigurationen durchführen.

TIPP 3:

Machen Sie sich klar, wer die “VIPs” in Ihrer Organisation sind.

Oft ist zum Beispiel Programmierer:innen oder IT-Mitarbeiter:innen nicht klar, dass sie aus IT-Sicht sehr viele Privilegien erhalten. Diese Personen sollten in ihrem Handeln und in ihrer Ausbildung entsprechend sensibilisiert werden.

#TIPP 4:

Kostenlose Online-Videoberatung der WKO

Nutzen Sie die monatlichen Digitalisierungs.BERATUNG und besprechen mit Expert:innen Ihre IT-Sicherheitsthemen sowie Fördermöglichkeiten für die Umsetzung. Digitalisierungs.BERATUNG - WKO.at

#TIPP 5:

Wissen ist Schutzschild – Top-Experten-Know-How für Sie vor Ort

Eine sichere EDV, aufmerksame Mitarbeiter: innen und aktuelles Wissen sind das wertvollste Schutzschild - ebenso praxisorientierte Informationen von Sicherheitsexperten rund um das Thema "Cyber-Security“. Die WKO-Bezirksstellen bringen die Experten kostenlos zu Ihnen in die Region:

Alle Termine und Anmeldung unter:

Digital vernetzt und ausspioniert - Sind Sie sicher, dass Sie sicher sind?