Licht und Schatten der Digitalisierung

BILD: KRAN77-STOCK.ADOBE.COM

Schlagzeilen wie „Hacker verschaffen sich Zugang zu über 160.000 Nintendo-Accounts“[1] oder auch Aussagen wie die des Bitkom-Präsidenten Achim Berg „Umfang und Qualität der Angriffe auf Unternehmen haben dramatisch zugenommen“[2], lassen einen hellhörig werden.

Ist es um die IT – Sicherheit, die Informationssicherheit und den Datenschutz in Deutschland wirklich so schlecht bestellt? Und wenn ja, warum unternehmen die CIOs, CTOs, CISOs, DSBs, COs... nichts dagegen?!

Um diese Fragestellungen in das richtige Licht zu rücken, sollte zunächst einmal hinterfragt werden, welche Kriterien bzw. Rahmenparameter die sogenannten „Entscheider“ überhaupt haben. Das große Schlagwort unserer Zeit lautet „Digitalisierung“. Hinter diesem Schlagwort verbergen sich aber nicht nur geänderte technologische Anforderungen, sondern auch gesellschaftliche Veränderungen. Heute ist es fast selbstverständlich von einem beliebigen Endgerät aus, sei es Notebook, Smartphone, Tablet etc. von fast jedem Ort auf dieser Welt seinen Kalender einzusehen, Mails zu checken oder daheim – wie Smart Home – digital mal kurz nach dem Rechten zu schauen.

Für die IT-Sicherheit, oder Neudeutsch: die Cybersecurity, ergeben sich aber allein aus diesem geänderten Nutzerverhalten dramatisch neue Herausforderungen. Wo früher der Zugang zu einem Unternehmen mit möglichst hohen Zäunen und effektiven Firewalls abgeschottet wurde, hat man heute das Problem, dass sich die Mitarbeiter*innen leider nicht mehr nur in dieser „geschützten und kontrollierbaren“ Firmenumgebungen aufhalten. Mobiles Arbeiten und Homeoffice sind an der Tagesordnung, und damit haben sich diese ursprünglich starren und kontrollierbaren „Grenzen“ – man spricht auch vom Perimeter – nicht nur verschoben, nein, sie sind quasi genauso mobil und flexibel wie der Mensch dahinter. Um diese „neue Freiheit und Flexibilität“ richtig genießen zu können / zu leben, gibt es ja auch noch eine Vielzahl an vielversprechenden Tools, wie z. B. Dropbox, GoogleDocs, S3 Buckets. All diese Dinge haben eines gemeinsam: Sie basieren auf der Nutzung einer Cloud bzw. einer cloudähnlichen Konstruktion.

Betrachten wir diese Use Cases etwas genauer. Was haben sie alle gemeinsam?

a) Hat sich der sogenannte Perimeter verschoben – hin zum Endgerät?

b) Benötigen alle Komponenten eine konstante Verbindung ins Internet oder neutral formuliert, in das Netz, über welches die Services erreicht werden?

c) Sind die Informationen und Daten nicht mehr für sich abgeschottet im Hochsicherheitsbereich ablegbar, sondern müssen für den User – weltweit – transparent verfügbar sein?

Mit dieser Zusammenfassung haben wir auch die drei Felder, auf die eine intakte IT-Security oder Cybersecurity-Einheit Antworten geben sollte:

a) Wie werden beliebige Endgeräte geschützt?

b) Wie kann eine sichere Verbindung / Netzwerkverbindung von fast jedem Ort dieser Welt hergestellt werden?

c) Wie können die Möglichkeiten z. B. einer Cloud-Lösung sicher und datenschutzkonform, im Sinne von TOMs, eingebunden werden?

Auf diese Vielzahl von Fragen Antworten zu finden und unter dem Druck des Marktes, immer schneller und günstigerer Produkte zu liefern, sei es Software aber auch Hardware, stellt eine Herausforderung dar.

Gerne unterstützen wir Sie bei der Beantwortung dieser Fragen und bei der Umsetzung.

Tobias Birk
Geschäftsfeldleiter Security Solutions der PROFI Engineering Systems AG

BILD: PROFI ENGINEERING SYSTEMS AG

PROFI
Innovative IT-Lösungen

Weitere Informationen erhalten Sie unter: https://www.profi-ag.de/

1 https://www.datenschutzticker.de/2020/04/hacker-verschaffen-sich-zugang-zu-ueber-160-000-nintendo-accounts/

2 https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr