„GANZHEITLICH DENKEN“

Die Berliner Security- und IT-Managementberatung HiSolutions AG ist auf den Schutz digitaler Prozesse spezialisiert. Vorstandsmitglied Prof. Timo Kob rät Unternehmen, ihre Security-Konzepte zügig an eine neue Arbeitswelt mit hohen Homeoffice-Anteilen anzupassen.

AUTOR: PETER TRECHOW

Wie hat Ihr Unternehmen den Lockdown während der Corona-Krise gemeistert?

Als IT-Beratung haben wir keine Maschinen und stationäre Infrastruktur, an der unsere Arbeit hängt. Hinzu kamen zufällig günstige Voraussetzungen: Wir haben vor zwei Jahren entschieden, unsere 200 Mitarbeiter mit Notebooks auszustatten und Desktop-PCs abzuschaffen. Auch fiel der Lockdown mit einem geplanten Umzug zusammen. Mobiles Arbeiten war ohnehin eingeplant. Und ein Gutteil des Umzugs hat sich erledigt, indem Mitarbeiter ihre ergonomischen Büromöbel ins Homeoffice mitnahmen. Wie es der Zufall wollte, waren wir auch theoretisch fest im Sattel: ▸

Zur Person

Prof. Timo Kob ist Mitbegründer und Vorstandsmitglied der HiSolutions AG in Berlin und stellvertretender Vorstandsvorsitzender des Bundesverbandes Allianz für Sicherheit in der Wirtschaft e.V. (ASW)..

Im Rahmen unserer Beratungstätigkeit und meiner Professur bin ich seit 14 Jahren in der Pandemieplanung aktiv. Cyber-Security und betriebliche Kontinuitätsplanungen greifen in so einer Situation direkt ineinander. Das haben wir alle nun auch praktisch erfahren.

Hatten Sie Sorge, sich mit der dezentralen Arbeit im Homeoffice neue Cyber-Risiken einzuhandeln?

Da wir an den Themen E-Government und Cyber-Security arbeiten und viel für das Bundesamt für Sicherheit in der Informationstechnik (BSI) tätig sind, agieren wir ohnehin auf hohem Sicherheitsniveau. Alle Notebooks haben verschlüsselte Festplatten und sind über sichere VPN-Zugänge vernetzt. Wir mussten in der Krise nur unsere VPN-Kapazitäten hochfahren, weil plötzlich alle Mitarbeiter mobil arbeiteten. Unsere Herausforderung war eher, dass Kunden Probleme hatten, genug Tokens, also Zugangsberechtigungen, für ihre VPN-Netzwerke zu beschaffen. Verfügbare Tokens gingen an eigene Mitarbeiter und wir waren außen vor. Der Markt für hardwarebasierte Sicherheitslösungen war ebenfalls in kürzester Zeit leergefegt. Wir haben Kunden dann teils sogar unbezahlt arbeitsfähig gemacht, um unser Projekte weiterführen zu können.

Was heißt es für Security-Strategien von Unternehmen, wenn viele Mitarbeiter im Homeoffice arbeiten?

Mobile Geräte und VPN sind Basics, ohne die es nicht geht. In manchen Unternehmen arbeiten Mitarbeiter an Privat-PCs und versenden sensible Daten unverschlüsselt per Mail. Da tun sich gravierende Sicherheitslücken auf. Um mobiles Arbeiten und die Vernetzung von Maschinen auf sichere Füße zu stellen, sind ganzheitliche Sicherheitsarchitekturen gefragt. Ob klassische Desktop-PCs darin Zukunft haben, ist fraglich. Denn mit zentral gemanagten, verschlüsselten Notebooks bin ich 80 Prozent aller Sorgen los – und zugleich flexibel. Büroarbeit wird künftig vermehrt dem fachlichen und menschlichen Austausch in Teams dienen, der beim Lockdown zu kurz kam. Wenn Büroarbeitszeit vor allem dazu dient, unterschiedlich zusammengesetzte Teams zu treffen, wird mobiles Arbeiten auch hier immer wichtiger.

Mit Corona schlägt die Stunde der Cloud-Services. Was gilt es dabei aus Ihrer Sicht zu beachten?

Die verschiedenen Webkonferenz-Anbieter und Datenaustauschplattformen nehmen sich in puncto Security nicht so viel wie es mancher Medienbericht suggeriert. Jüngere Anbieter hatten anfangs Sicherheitslücken, sind aber transparent und konstruktiv damit umgegangen. Problematischer sind ungeschulte Anwender. Es gab Fälle öffentlich sichtbarer Meetings. Wer nicht weiß, welche Sicherheitseinstellungen es gibt, kann die Häkchen nicht an richtiger Stelle setzen. Cloudnutzer sollten sich über sichere Konfigurationsmöglichkeiten informieren. Und sie sollten Versprechen einer End-to-End-Verschlüsselung hinterfragen. Denn die Anbieter legen diese teils sehr unterschiedlich aus. Sensible Informationen sollten zudem nicht über Server im Ausland laufen und möglichst nur in eigenen gekapselten Systemen verarbeitet werden.

Nun ist die Cloud im Industrial Internet of Things unverzichtbar. Heterogene IT-Systeme vernetzen immer mehr Maschinen, Mitarbeiter und Partner. Wie sehen Sie als Security-Experte diesen Trend?

Für die Verbindung von Information und Operation Technology (IT & OT) fehlen oft angemessene Security-Lösungen. Daher plädiere ich in solchen Fällen für die Trennung, selbst wenn es bedeutet, auf Funktionen zu verzichten. Es gibt ein geflügeltes Wort: „If it can kill you, don´t connect it". Wo immer möglich, sollten Sie beispielsweise Datenverkehr nur in eine Richtung erlauben und Zugriffe von außen unterbinden …

… was nicht wirklich mit Remote Services und Industrie-4.0-Plattformen kompatibel wäre.

Auch wenn der Satz in der vernetzten Produktion nicht durchzuhalten ist, sollte er die Richtschnur sein. Muss ein smarter Stromzähler wirklich die Stromabschaltung von außen ermöglichen? Ist es zwingend nötig, dass Mitarbeiter im Service-Helpdesk mobil arbeiten und auf jede Kundenmaschine weltweit zugreifen können? Bequem ja – aber notwendig? Jede Stufe der Vernetzung löst neue Risiken und Angriffspunkte aus. Daher gilt es, Nutzen und Risiken im Vorfeld abzuwägen und sinnvolle Kompromisse zwischen Funktionalität, Komfort und Sicherheit zu erarbeiten. Sicherheit muss von Anfang an mitgedacht werden. Sie ist kein Add-on, an das man kurz vor Einführung denken kann. Aber wer sie sauber konzipiert, kann sehr viel machen.

Mit zentral gemanagten, verschlüsselten Notebooks ist man im Homeoffice 80 Prozent der Sorgen los.

Fotos: Dario Lehner / vor-ort-foto.de

„Wo immer möglich, sollte man Zugriffe von außen unterbinden."

PROF. TIMO KOB

Manche internationale Regierung erschwert verschlüsselte VPN-Datenübertragungen. Welchen Einfluss hat das politische Umfeld auf die IT-Security?

IT-Security ist eine politische Spielwiese. Großmächte in Ost und West betreiben Wirtschaftsspionage und überziehen ihre Bevölkerung und ausländischen Besucher mit Kontrollen im digitalen Raum. Wir empfehlen Kunden bei Reisen in kritische Regionen fabrikneue Mobilgeräte ohne Daten mitzuführen und halten es selbst so. Auch in der EU gibt es Stimmen, die zur Terror- und Kriminalitätsabwehr am liebsten Verschlüsselungen verbieten würden. Doch wir wissen, dass Anschlagsplanungen dann eben in Chats von Playstation und Online-Games laufen. Solche Ausweichmöglichkeiten haben Unternehmen beim Schutz vor Spionage und Cyber-Attacken nicht. Verschlüsselungsverbote schaden den „Guten", ohne die „Bösen" zu treffen.

Kann künstliche Intelligenz IT-Systeme absichern oder umgekehrt als Waffe für hochwirksame Angriffe dienen?

Beides findet statt. Security-Anbieter und Kriminelle befinden sich im Wettbewerb um die effektiveren KI-Algorithmen. Die einen suchen mit KI Anomalien und lassen KI-Systeme gegeneinander antreten, um sie besser zu verstehen und aneinander zu trainieren. Die anderen suchen damit Sicherheitslücken. Bei alledem tut sich ein Problem auf: Selbst Experten können kaum noch nachvollziehen, wie Antworten von KI zustande kommen und wie sinnvoll sie sind. Teils fühle ich mich an Goethes Zauberlehrling erinnert. Wir sind von der Komplexität vernetzter Systeme überfordert und verstehen die Algorithmen nicht mehr, die sie absichern. Möglicherweise werden künftige Generationen die frühen 2020er nicht nur mit Covid-19 verbinden, sondern sie als Zeitalter großer digitaler Naivität bewerten.

Steffen Zimmermann
Telefon +49 69 6603-1978
steffen.zimmermann@vdma.org

Link für xxxx
go.vdma.org/xxxxx