Ausgabe 28 – Oktober 2020 – **Herausgegeben vom TAGEBLATT**

BUSINESS & PEOPLE

DAS WIRTSCHAFTSMAGAZIN AUS DER METROPOLREGION HAMBURG

INTERVIEW

Corona: Channel-Begründer Arne Weber rät zu Vorsicht und Besonnenheit

Seite 2

B&PIMPACT

Wohin mit meinem Geld? Das sagen die Anlage-Experten

Seiten 4+5

PRODUKT

Inklang-Chef Thomas Carstensen bringt „AYERS“ auf den Markt

Seite 8

DER MARKT BOOMT: DAS IMMOBILIEN-SPECIAL 2020

WARTEN AUF DIE GENERATION Z

New Work stellt alles auf den Kopf

Covid-19 wirkt in vielen Unternehmen wie ein Katalysator – Homeoffice ja oder nein? – Auswirkungen auch auf die Baubranche

Von Wolfgang Becker

Nach dem B&P-Gespräch mit Herbert Schulte und Pamela Reidt von Dierkes Partner stand fest: Das Thema gehört auf den Titel. Die Personalleiterin hatte soeben erläutert, wie sich die Hamburger Partner-Kanzlei (Wirtschaftsprüfer, Steuerberater, Rechtsanwälte) auf die Zukunft des Arbeitens einstellt und dabei Gedanken formuliert, die manchem Unternehmer den Atem rauben dürften. Zum Beispiel: 20 Stunden Arbeit bei 40 Stunden Gehalt, Anfangszeiten selbst bestimmen, Mobilitätssicherung, keine Anwesenheitspflicht und so weiter – eine Liste mit zwölf Punkten, die ein Bild davon zeichnet, wie die Arbeitswelt in fünf Jahren aussehen könnte. Steuerberater Herbert Schulte: „Die viel zitierte Work-Life-Balance ist in der kommenden Mitarbeitergeneration viel präsenter – darauf müssen wir uns als Arbeitgeber einstellen.“ New Work ist das Stichwort.

HBI hat den Plan

Der Vormarsch der Homeoffice-Bewegung wirkt sich sogar auf Investments und Gebäudeplanungen aus. Zum Beispiel in Neu Wulmstorf: Direkt an der S-Bahnstation baut die HBI Hausbau-Immobiliengesellschaft aus Nottensdorf jetzt ein Büro- und Dienstleistungszentrum – eine strategische Entscheidung, denn bislang war Neu Wulmstorf nicht als Bürostandort auf der Landkarte zu finden. Aber: Die Gemeinde liegt auf der Hauptpendlerstrecke zwischen Stade und Hamburg. Das HBI-Konzept sieht den Bau flexibler Büroflächen vor, die im Zeichen von New Work stehen sollen und vor allem eines sind: gut erreichbar.

„Das regelt die Praxis“

Die Pandemie arbeitet wie ein Katalysator. Mark Behr, Innovationsmanager im hit-Technopark, rechnet damit, dass auch die 110 Mieter künftig weniger Platzbedarf haben werden – die Unternehmensstruktur im Technologiepark dürfte dementsprechend kleinteiliger werden. Falko Junge, Unternehmensberater in der Kanzlei Schlarmann-von-Geyso, sagt: „Die Corona-Krise legt strukturelle Defizite ganz deutlich offen. Da geht es um konkrete Punkte wie Teile-Produktion in China und daraus entstehende Abhängigkeiten, digitale Arbeitswelten, neue Arbeitsprozesse – Stichwort New Work – und vieles mehr.“

Es gibt aber auch andere Zwischentöne: Der AGA Unternehmensverband kommt im Rahmen einer Studie zu diesem Ergebnis: „Unsere Warenwelten und Dienstleistungen lassen sich nicht vollständig aus dem Homeoffice bewegen. Nicht jede Tätigkeit ist Homeoffice-fähig“, mahnt Hauptgeschäftsführer Volker Tschirch. Thomas Falk, Hauptgeschäftsführer des Arbeitgeberverbandes Stade Elbe-Weser-Dreieck e.V., warnt davor, das Recht auf Homeoffice gesetzlich zu fixieren: „Das regelt die Praxis.“ Auswirkungen auf die Baubranche erwartet der Harburger Bauunternehmer und Investor Arne Weber: „Ich denke, es wird erst mal grundsätzlich weniger gebaut werden.“

Mehr zum Thema lesen Sie auf den Seiten 2, 3, 15, 16 und 18 sowie im Immobilien-Special auf den Seiten 13, 16 und 31.

IT-SECURITY

Tedesio weiß, wie sich der digitale Daten-GAU vermeiden lässt **Seite 20**

IM- UND EXPORT

Vitaminstrom: Hier trifft Elbe-Obst auf den Global Fruit Point **Seite 21**

DER B&P-NEWSLETTER

Hamburg und Bremen? Das geht! Im neuen B&P-Newsletter, der auf Wunsch einmal im Monat zugeschickt wird. Kostenlose Anmeldung unter

» **https://www.business-people-magazin.de/newsletter/**

So verhindern Sie den digitalen SuperGau

Was tun, wenn plötzlich alle Daten weg sind? Gabriele Fricke und Jörg Ertel von Tedesio in Buchholz geben Antwort

„Der Feind von innen“

Firma X, ein IT-Dienstleister und Hardware-Händler aus Norddeutschland, beschäftigt 40 Mitarbeiter. Der größte Kunde wirbt einen Mitarbeiter ab und will die Dienstleistung künftig intern regeln. Die Abgeworbene löscht am letzten Arbeitstag alle Daten seines künftigen Arbeitgebers und zusätzlich das Backup. Seinen Rechner setzt er komplett neu auf. Folge: Firma X hat alle Daten des Hauptkunden verloren.

Jörg Ertel: „Fragen an uns: Können die Daten wieder hergestellt werden? Von welchem Gerät wurde der Löschvorgang ausgelöst? Ziel war es natürlich, den Täter zu überführen. Kurz: Nach gut drei Tagen waren etwa 90 Prozent der Daten wieder da. Wir konnten den Rechner identifizieren und eindeutig zuordnen. Der Auftraggeber erhielt von uns ein gerichtsfestes Gutachten.“

TIPP 1: Wenn Daten gelöscht wurden, muss sofort gehandelt werden. Löschen bedeutet im Grunde nur, dass der Sektor auf dem Speichermedium (Festplatte) zum Überschreiben freigegeben wird. Was als gelöscht markiert ist, kann bei schnellem Handeln dennoch widerhergestellt werden.

„Der Feind von außen“

Firma Y ist ein deutschlandweit tätiges Logistikunternehmen und durch einen Verschlüsselungstrojaner lahmgelegt. Hacker verlangen ein Lösegeld, bevor die Daten wieder freigeschaltet werden.

Jörg Ertel: „Das Unternehmen hatte Glück, denn die Datensicherung war nicht ans System angeschlossen, und es lag auch noch eine Papierform vor. Die Touren konnten also weiterhin gefahren werden. Wir haben das Netzwerk analysiert, aufgedeckt, über welchen Computer der Trojaner ins Unternehmen kam, und die Mailadresse gefunden, über die ein Backdoor-Programm eingeschleust worden war. Durch die offene Hintertür kamen die Hacker ins System und schauten sich erstmal um. Der Verursacher kam aus dem außereuropäischen Ausland. Wir haben die Mitarbeiter einer intensiven Schulung unterzogen, eine Netzwerküberprüfung durchgeführt und Schutzmaßnahmen definiert.“

TIPP2: Es sollten regelmäßig Backup-Kopien erstellt und räumlich getrennt (!) vom System verwahrt werden.

TIPP 3: USB-Sticks beispielsweise mit Kundendateien stets in einer isolierten Umgebung öffnen. Aktuelle Betriebssysteme haben im Regelfall ein Sicherheitssystem integriert (beispielsweise das Microsoft-Programm „Sandbox“). Ein Virenscanner allein reicht nicht aus.

Spionage, Erpressung, Freude an destruktiven Aktionen oder auch einfach nur Chaos in der eigenen IT-Infrastruktur – es gibt viele Gründe, warum Daten blockiert, gestohlen oder gelöscht werden. Cyberkriminalität ist ein Thema, von dem selbst gut aufgestellte große Unternehmen nicht verschont bleiben, wie das aktuelle Beispiel der Uniklinik Düsseldorf zeigt. Jörg Ertel, Informatiker, Dekra-Sachverständiger und BSI-Grundschutzexperte, ist CISO (Chief Information Security Officer) beim bundesweit tätigen IT-Dienstleister Tedesio. Er hat regelmäßig mit Unternehmen zu tun, die entweder gehackt wurden und nun versuchen, ihre Daten wieder herstellen zu lassen und den Daten-Klau zurückzuverfolgen (Forensik), oder aber Beratung brauchen, wie der digitale SuperGau verhindert werden kann (IT-Security). Mit ihm und Vertriebschefin Gabriele Fricke sprach B&P über drei konkrete Gefahrenlagen: „den Feind von außen“, den „Feind von innen“ und den besonderen Fall, wenn Unternehmer überrascht feststellen: „Der Feind bin ich!“

Wenn selbst der Bundestag gehackt werden kann, ist eigentlich schon klar, dass die Hacker-Szene vor nichts zurückschreckt. Die Zahl der Firmen, deren Daten durch eingeschleuste Schadsoftware verschlüsselt werden, steigt offenbar stetig an. Solche Angriffe enden in der Regel mit Lösegeldforderungen und verzweifelten Versuchen, doch noch irgendwie an die Daten heranzukommen und die Systeme wieder hochzufahren. Unter dem Dach des Bundesinnenministeriums sitzt das bereits 1991 gegründete Bundesamt für Sicherheit in der Informationstechnik (BSI). Jörg Ertel: „Dort wird zurzeit die Cyberwehr aufgebaut.“

Es sind aber nicht immer Angriffe von außen, die Unternehmen gefährlich werden können. Ertel: „Das größte Gefahrenpotenzial sind nach wie vor unvorsichtige Mitarbeiter, die unwissentlich oder im schlimmsten Fall fahrlässig die Türen ins System öffnen. Da reicht schon ein Klick auf eine unerkannte Phishing-Mail oder ein fremder USB-Stick. Häufig liegen die Ursachen aber auch in organisch gewachsenen IT-Strukturen mit Rechnern, die den aktuellen Anforderungen an Sicherheit nicht gewachsen sind.“ Allerdings sagt der Experte auch: „Es gibt keine absolute Sicherheit, aber eine individuelle Beratung und ein entsprechendes Konzept hilft, Schäden abzuwenden.“

Tedesio ist in der Lage, auch komplexe Rechnersysteme zu durchforsten – zum einen, um verlorene Daten doch noch aufzuspüren; zum anderen, um den Weg zurückzuverfolgen, den beispielsweise ein Verschlüsselungstrojaner ins Unternehmen gefunden hat. Gabriele Fricke: „Wir schauen uns die Systeme an und scannen die Schwachstellen. Das gilt natürlich auch für Unternehmen, die sich prophylaktisch schützen wollen. In diesen Fällen können wir beispielsweise Hackerangriffe simulieren und die gefundenen Schwachstellen anschließend beheben. Wir bieten einen individuellen Security-Check an und erstellen Sicherheitskonzepte. Kommt es zum Schaden, schreiben wir auch gerichtsfeste Gutachten.“

Tedesio beschäftigt bundesweit 38 Mitarbeiter, darunter etwa ein Dutzend im Raum Hamburg. Die Zentrale ist in Buchholz. Alle Mitarbeiter sind festangestellt und arbeiten dezentral. Die Kunden lassen sich überwiegend dem Mittelstand zuordnen. wb

Gabriele Fricke und Jörg Ertel sind beide Mitglieder der Geschäftsführung des Buchholzer Unternehmens Tedesio.

Foto: Wolfgang Becker

» **Web: www.tedesio.de**

„Der Feind bin ich“

Firma Z verfährt nach dem Prinzip „Never touch a running System“ – die IT-Architektur ist seit Jahren gewachsen, der Operator ist in die Aufgabe hineingewachsen, aber nicht wirklich auf dem neuesten Stand. Die Kosten für eine Neuaufstellung der IT wurden bislang gescheut, denn es lief ja immer alles.

Jörg Ertel: „In den Augen vieler Unternehmer hat die IT noch nicht die Priorität, die ihr zukommen sollte. Häufig werden nur die Kosten gesehen. Wird das Thema vernachlässigt, droht irgendwann der DatenGau. Unverzichtbar ist zum Beispiel ein gutes Backup-Konzept. Die Datensicherung sollte regelmäßig auf ihre Funktion überprüft und dokumentiert werden – für den Schadensfall. Neue Mitarbeiter müssen detaillierte Infos bekommen, wie sie mit Daten umzugehen haben. Gewachsene Strukturen führen oft dazu, dass viel zu viele User Zugriff auf Daten haben. Wer definiert die Rechte? Wer darf alles im Wlan-Netz angeschlossen sein? 80 Prozent der mittelständischen Unternehmen gewähren zu viele Zugriffsrechte. Manchmal finden wir Benutzer, die schon lange nicht mehr im Unternehmen beschäftigt sind. Niemand hat ihren Account geschlossen, geschweige denn deinstalliert. Es kommt sogar vor, dass Mitarbeiter im Homeoffice die Buchhaltung auf ihren privaten Rechnern erledigen. Wenn Unternehmen hier nachlässig sind, öffnen sie Missbrauch und Cyberattacken Tür und Tor – so werden sie zu ihrem eigenen Feind.“

TIPP 4: Netzwerke sollten unbedingt segmentiert werden. Der Klassiker: die strikte Trennung von Firmen-Wlan und Gast-Wlan.

TIPP5: Mitarbeitern sollten niemals eigenständig Programme aus dem Internet auf ihre Dienstrechner laden können.