IMPULS/

No14 JULI 2021

MARTENS/PRAHL/SICHER SEIN

DAS MARTENS & PRAHL KUNDENMAGAZIN

WENN „DIE WOLKEN“ BRENNEN, SIND AUCH DATEN IN GEFAHR

Im März 2021 ist das größte Rechenzentrum Europas in Flammen aufgegangen und mit ihm die Daten vieler Unternehmen. Mehr auf Seite 2

HINWEIS ZUM THEMA GENDERING:
Aus Gründen der besseren Lesbarkeit wird im Folgenden auf die gleichzeitige Verwendung männlicher, weiblicher und diverser Sprachformen verzichtet. Sämtlich Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

PROJEKT ZUKUNFT: WIR SETZEN AUF NACHHALTIGKEIT

Der Klimawandel ist kein Risiko der Zukunft, sondern bereits Realität. Darum übernehmen wir in der MARTENS & PRAHL Holding Verantwortung und tragen aktiv zur Reduktion von CO_2-Emissionen bei. Unser Maßnahmen-Konzept, das auf Basis der Analyse von First Climate von unserem Team entwickelt wurde, umfasst Lösungen für alle Arbeitsbereiche.

MARTENS/PRAHL/KLIMAGRÜN

Mehr über unsere Nachhaltigkeits-Strategie erfahren Sie hier:
www.martens-prahl-holding.de/service/presse-center/klimagruen

DAS PRAXISBEISPIEL

WENN „DIE WOLKEN“ BRENNEN, SIND AUCH DATEN IN GEFAHR

Die Vorstellung, dass unsere Daten in einer „Cloud“, einer „Wolke“, sicher gespeichert, nicht angreifbar und unlöschbar sind, ist demnach also nicht ganz korrekt, so dass sich Unternehmen die Frage stellen müssen, was sie tun und beachten müssen, um die Sicherheit ihrer Daten zu gewährleisten. Und hier schon einmal vorab: Eine hundertprozentige Sicherheit gibt es nicht. Für Unternehmen geht es darum, Risiken zu minimieren oder besser zu vermeiden und im besten Fall die Restrisiken über eine Versicherung abzusichern.

Dass die Daten sicher und dank der Cloud auch dann noch verfügbar sind, wenn ein Rechner kaputt geht oder gestohlen wird, ist ein Werbeversprechen der Anbieter, welches jedoch die Unternehmen nicht von ihrer Pflicht entbindet, sich auch weiterhin Gedanken über eine Sicherung ihrer Daten machen zu müssen

Der Brand bei Europas größtem Cloud-Anbieter OVH, bei dem ein fünfstöckiges Rechenzentrum den Flammen zum Opfer gefallen ist und auch Backup-Server zerstört wurden, macht einmal mehr die verheerenden Folgen für Unternehmen sichtbar: Online-Dienste und Websites waren nicht mehr verfügbar und viele Kunden haben ihre Daten teilweise oder sogar komplett verloren.
Suggerieren wir Ihnen als Unternehmen, Cloud Services künftig nicht mehr zu nutzen? Mitnichten! Cloud Services erfreuen sich zu Recht immer größerer Beliebtheit, dennoch ist es wichtig, dass Unternehmen die Frage „Wie sicher ist (m)eine Cloud?“ beantworten müssen, um eine korrekte Risikoeinschätzung vornehmen zu können. Um hierauf eine Antwort zu finden, müssen Unternehmen und Cloud-Anbieter sich ihrer Aufgaben und Pflichten bewusst sein, damit die größten Schätze unseres Informationszeitalters so sicher wie möglich verwahrt sind.

Genug der Theorie – kommen wir zu einem praktischen Beispiel:

Die Firma Meisel Pumpenbau GmbH nutzt OVHcloud, um standortübergreifend auf ihre Daten zugreifen zu können. Die Cloud bietet ihnen viele Vorteile: Kosten für die eigene Hardware können ebenso wie Speicherplatz je nach Bedarf zeitnah vergrößert oder verkleinert werden.

Im Falle von Schäden an der eigenen Festplatte oder durch einen Blitzeinschlag mit Überspannungsschäden gehen keine Daten vor Ort verloren. So hat sich mit der Auslagerung der Daten in der Cloud – fernab irdischer Risiken – nicht nur ein vermeintlich gutes Gefühl beim Unternehmen eingestellt, dass die Daten sicher verwahrt sind, sondern auch die Meinung, dass die Verantwortung für die Sicherheit der Daten von Meisel Pumpenbau nunmehr beim Cloud-Anbieter OVH läge.
Arbeitsstart Donnerstag früh. Als die Mitarbeiter ihre Rechner einschalten, bleiben die Bildschirme schwarz, es kann keine Verbindung zur Cloud aufgebaut werden. Das hat Folgen und vor dem geistigen Auge des Unternehmers entwickelt sich folgendes Szenario:

1. Die Mitarbeiter haben keinen Zugang auf die Systeme.
2. Gegenüber Kunden und Lieferanten ist das Unternehmen nicht mehr auskunftsfähig.
3. Die Prozesse im Unternehmen funktionieren nicht mehr.
4. Die Kundenzufriedenheit sinkt.
5. Aufträge können nicht mehr zeitgerecht bearbeitet werden.
6. Vertragsstrafen drohen.
7. Der Umsatz sinkt.
8. Die Existenz des Unternehmens ist gefährdet.
9. Mitarbeiter müssen entlassen werden.

Doch bevor und damit diese Visionen nicht Realität werden, nimmt Meisel Pumpenbau Kontakt mit OVH auf, um zu klären, wann die Datensicherungen des Unternehmens wieder eingespielt sind und das Unternehmen weiterarbeiten kann.

Zwei Tage dauert es, bis das Unternehmen jemanden beim Cloud-Dienstleister erreichen kann und man erklärt im Telefonat, dass laut Vertrag keine Datensicherungen vorgesehen waren. Für den Baustein „Datensicherung in einem separaten Rechenzentrum“ hätte man eine kostenpflichtige Erweiterung bestellen müssen. Das Unternehmen hatte sich auf die Cloud verlassen und war – fälschlicherweise – davon ausgegangen, dass eine Datensicherung als standardmäßige Leistung im gebuchten Leistungsumfang enthalten sei. Ein teurer Trugschluss, wie sich herausstellt, denn das Unternehmen hatte selbst keine eigene Datensicherung angefertigt.

Fakt ist, wir haben hier ein Unternehmen mit über 100 Mitarbeitern, welches bereits seit 28 Jahren am Markt ist. Sie tragen keinerlei Verantwortung für den Brand beim Cloud-Anbieter und können aufgrund ihres Vertrages keinen Regress nehmen. Mit schwerwiegenden Folgen für das Unternehmen: Durch den Brand hat das Unternehmen gegen §§238 / 257 HGB, §147 AO und DSGVO verstoßen und muss für die rechtlichen Konsequenzen geradestehen, im schlimmsten Fall haftet der Geschäftsführer sogar mit seinem privaten Vermögen. Gerettet hat das Unternehmen die Tatsache, dass die Daten vollumfänglich in einem der anderen Rechenzentren lagen, die nur heruntergefahren waren. Diese Nachricht hat das Unternehmen aber erst Tage später vom Cloud-Anbieter erhalten. Nochmals Glück im Unglück gehabt!

Welche Handlungsempfehlungen können wir aus dem Brand bei OVH und dem skizzierten Beispiel ableiten? Als Unternehmer müssen Sie vor der Nutzung einer Cloud-Lösung zentrale Fragestellungen klären: Von der Einrichtung von Nutzer-Berechtigungen, über Datensicherheit und -sicherungen bis hin zum Thema „Was passiert im Schadenfall?“.

Für eine umfassende Beratung wenden Sie sich am besten an den Makler Ihres Vertrauens, der Sie über alle wichtigen Fragen rund um das Thema Cloud-Nutzung und Datenschutz informieren kann.

Nikolaus Stapels –
Geschäftsführer Vertriebssoftware24 GmbH und
Inhaber Nikolaus Stapels Consulting & Training

WIRTSCHAFTSKRIMINALITÄT

EU-HINWEISGEBER-RICHTLINIE: NEUE ANFORDERUNGEN FÜR UNTERNEHMEN

Deutschen Unternehmen entstehen jedes Jahr hohe Schäden durch Wirtschaftskriminalität. Straftaten, die durch Verdachtsmeldungen von Mitarbeitern im Unternehmen oft frühzeitig erkannt und zum Teil vermieden werden könnten. Zur Stärkung solcher internen Kontrollsysteme hat die EU eine neue Richtlinie erlassen, die sogenannte „Hinweisgeber-Richtlinie". Natürliche Personen sollen hierdurch besser geschützt werden, wenn sie Verstöße gegen geltendes Recht melden bzw. veröffentlichen wollen.

Ein Referenten-Entwurf zur Umsetzung in Deutschland liegt bereits vor und verpflichtet Unternehmen mit mindestens 250 Mitarbeitern bis voraussichtlich 17.12.2021, geeignete Meldekanäle einzurichten. Auch Unternehmen mit 50 – 249 Mitarbeitern wird diese Verpflichtung treffen; sie gilt aber für diese Zielgruppe erst nach einer verlängerten Übergangsfrist von zwei Jahren voraussichtlich ab 17.12.2023.

Herausfordernd sind vor allem die konkreten Anforderungen an die Meldekanäle:

So muss eine Meldung schriftlich oder mündlich möglich sein und auf Wunsch des Hinweisgebers auch ein persönlicher Austausch stattfinden können. Die Meldung soll allen Personen ermöglicht werden, die im Rahmen ihrer beruflichen Tätigkeit mit dem Unternehmen in Kontakt stehen – also eigene Mitarbeiter sowie Kunden und deren Mitarbeiter. Und die Informationen zu den Meldemöglichkeiten und weiteren Abläufen müssen klar und leicht zugänglich sein.

Besonders herausfordernd sind die geplanten Vorgaben für die Bearbeitung von Hinweisen:

Die Vertraulichkeit des Hinweisgebers muss über alle Meldekanäle gewahrt und unbefugter Zugriff Dritter ausgeschlossen werden. Dabei ist (natürlich) die DSGVO einzuhalten, also insbesondere der Schutz der personenbezogenen Daten aller beteiligten Personen – Hinweisgeber, Betroffene und Beobachter. Und sofern ein Betriebsrat vorhanden ist, hat mit diesem eine Abstimmung über die Einrichtung des Hinweisgeber-Systems zu erfolgen.

Für die betroffenen Unternehmen bedeutet dies in der Umsetzung insbesondere:

- Auswahl einer unparteiischen Person für die Bearbeitung der Meldungen,
- Konkretisierung der bei Meldungen zu ergreifenden Maßnahmen,
- Beachtung der Rückmeldefristen: Eingangsbestätigung innerhalb von sieben Tagen und eine Information über die ergriffenen Maßnahmen an den Hinweisgeber innerhalb von drei Monaten,
- eine Dokumentation der Vorgänge.

Betroffene Unternehmen stehen nun oft vor der Entscheidung, wie ein geeignetes Meldewesen umgesetzt werden kann.

Die Optionen für eigene Meldekanäle bringen unterschiedliche Herausforderungen mit sich:

So ist die Einrichtung eines Briefkastens oder Postfachs einfach umzusetzen. Die Wahrung der Anonymität ist aber nur erschwert zu gewährleisten, da Rückmeldungen an den Hinweisgeber erfolgen müssen. Ähnliches gilt für die Einrichtung von E-Mail-Postfächern mit Blick auf Zugriffsrechte der Administratoren und die Übermittlung von Meta-Daten. Bei einer eigenen Telefon-Hotline kann die erhöhte Hemmschwelle für Hinweisgeber kritisch werden und die Einrichtung von z. B. Chat-Bots bringt hohe technische Anforderungen mit sich.

Alternativ bietet sich die Beauftragung einer externen Ombudsperson oder die Nutzung einer Online-Plattform an. Ein möglicher Anbieter ist die Firma LegalTegrity[1], die als externer Dienstleister den Betrieb des Hinweisgebersystems inklusive Online-Plattform übernimmt.

Egal welchen Weg Ihr Unternehmen wählt: Effektive Meldekanäle sind ein wichtiger Beitrag für das eigene Risk-Management. Vor allem das Risiko von Schäden durch Vertrauenspersonen kann durch soziale Kontrollen im Unternehmen deutlich reduziert werden.

[1] https://legaltegrity.com

Julie Schellack –
MARTENS & PRAHL Holding

INTERNET-KRIMINALITÄT

CYBER-RISIKEN: DAS BEWEGT UNS HEUTE

Automatisierte Phishing-Angriffe, Internet of Behaviors, Social-Engineering, Cloud-Sicherheit und IT-Fachkräftemangel: Cyber-Kriminalität bleibt auch 2021 ein heißes Eisen. Es trifft nicht nur Unternehmen mit Lücken in der IT-Sicherheitsstruktur. Auch Kunden, die seitens ihrer IT-Sicherheitspolitik gut aufgestellt sind, melden zunehmend Schäden.

Das analoge Coronavirus beschleunigt kollektive Bemühungen zur Digitalisierung. Auch wenn COVID-19 in vielerlei Hinsicht ein Brennglas für defizitäre Zustände in der IT-Sicherheitskultur ist, grassiert das digitale Virus auch losgelöst von dieser Ausnahmesituation seit Jahren. Ganz gleich ob klein, mittel oder groß, rund 30 % aller deutschen Unternehmen[1] wurden in den letzten zwei Jahren Opfer einer Cyber-Attacke.

Hacker passen ihre Methoden permanent an optimierte Sicherheitsstandards an, Angriffsszenarien entwickeln sich weiter, die Gefahr verbreitet sich oft unbemerkt und unsichtbar.

Die Ursachen sind vornehmlich in der Digitalisierung zu suchen:

Die fortschreitende Digitalisierung macht Unternehmen immer anfälliger für Störungen der IT-Infrastruktur. Die Corona-Pandemie hat hier noch einen zusätzlichen Schub gegeben.

Teilweise konnten Sicherheits-Vorkehrungen mit der Digitalisierung nicht Schritt halten.

Es hat sich eine arbeitsteilige „Hacker-Industrie“ herausgebildet, die Unternehmen angreift. Angriffe werden also professioneller, die Folgen schwerwiegender.

Aktuell stechen vor allem drei Entwicklungen bei Hackern und Cyber-Attacken hervor. Ein Überblick:

1. Gut getarnt oder: Der Hacker als Sicherheitsforscher

Social-Engineering ist subtil, oft intelligent, aber nicht neu. Es zielt mittels zwischenmenschlicher Beeinflussung darauf ab, bei adressierten Personen ganz bestimmte Verhaltensweisen hervorzurufen. Die Preisgabe vertraulicher Informationen etwa, der Kauf eines Produktes oder die Freigabe von Finanzmitteln. Logisch, dass Hacker vor dieser effektiven Methode nicht Halt machen. Wie wirksam Social-Engineering-Angriffe sind, zeigt ein aktueller Vorfall, vor dem Googles Sicherheitsabteilung TAG (Threat Analysis Group) im Januar erstmals warnte. Demnach soll eine in Fernost vermutete Hacker-Gruppe Sicherheitsforscher ausspionieren – und zwar auf nie dagewesene Weise: Indem sich die Hacker selbst als aktive Forscher und Cybersecurity-Berater ausgaben, konnten sie sich über Monate das Vertrauen der vermeintlichen Kollegen erschleichen und für ihre Zwecke ausnutzen. Der Angriff macht deutlich, wie fragil der Faktor Mensch ist und wie wirksam gut vorbereitete Social-Engineering-Angriffe sind. Der von Google aufgedeckte Vorfall ist damit Warnung und Weckruf zugleich, die Standards in der Sicherheitsbranche zu überprüfen.

2. Richtig dicke Fische: Datenklau gefährdet alle Brasilianer

Nicht erst seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) in Europa ist Datenklau eine ständige Bedrohung für mittelständische und große Unternehmen. Einmal mehr, weil die Folgekosten wie Bußgelder, Benachrichtigungskosten und erpresserische Lösegeldforderungen steigen. Dass fremde Datensätze in fremde Hände gelangen, ist bekannt und davon abgesehen auch schnell passiert.

Neu hingegen ist die Entwicklung, dass Angreifer Datensätze in ganz großem Stil, nämlich in Form gigantischer Datenbanken, kopieren. Gigantisch meint in diesem Zusammenhang, dass dabei alle Grenzen, die beim herkömmlichen „Datenschaden“ allein durch Speichervermögen und Begrenzungen von E-Mail-Anhängen gegeben sind, überschritten werden. So wurde Anfang des Jahres 2021 bekannt, dass 220 Millionen Datensätze in Brasilien mit Namen, Geburtsdaten und Steuernummern geleakt wurden. Der Hack betrifft die gesamte steuerpflichtige Bevölkerung, was den Faktor Benachrichtigungsaufwand in absurde Höhen treibt und Unternehmen um ihre Existenz bringen könnte. Den Angriff hat das brasilianische Labor für Cyber-Sicherheit PSafe[2] aufgedeckt. Betroffen sind demnach auch Informationen über Unternehmen und Behörden.

3. Schreck statt Schutz: Firewall-Hersteller als Sicherheitsleck

Geschickte Hacker haben bislang unveröffentlichte Schwachstellen in SonicWall-Produkten ausgenutzt, um in die Systeme des Herstellers einzudringen. Die Cybersecurity Company SonicWall Inc.[3] spricht von einer koordinierten, „highly sophisticated[4]“, Attacke, die sich durch eine ganz besondere „Qualität“ auszeichnet: Werden bei neu entdeckten Schwachstellen in Sicherheitsprodukten üblicherweise die Kunden dieser Produkte angegriffen – und zwar so lange, bis diese mit einem Patch reagieren können – wurde hier in aller Sorgfalt und ohne viel Staub aufzuwirbeln der Hersteller selbst zum Opfer, denn natürlich setzt dieser auch die eigenen Produkte ein. Ein anderes, ähnliches, Beispiel war der Angriff auf die Microsoft Exchange-Server durch die Hacker-Gruppe Hafnium.
So ist dann auch die Schadenbelastung der Versicherer in den letzten 12 Monaten dramatisch gestiegen, speziell die Großschäden haben deutlich zugenommen. Neben Preissteigerungen und Kapazitätsverknappungen reagiert die Versicherungswirtschaft mit einer deutlichen Steigerung der geforderten Risikoinformationen – der Umfang der zu beantwortenden Risikofragen hat sich fast verdoppelt. Auch wenn sich diese teilweise nach Branchen und/oder Kundengröße staffeln und von Versicherer zu Versicherer unterschiedliche Schwerpunkte gesetzt werden: Ohne Bestätigung des Kunden, dass er relevante Sicherheitsmaßnahmen umgesetzt hat, bieten die Versicherer keinen Versicherungsschutz mehr an. Dazu zählen in der Regel folgende Maßnahmen:

- Es sind keine IT-Alt-Systeme (= nicht mit Sicherheitsupdates versorgte Systeme) vorhanden oder diese sind komplett gekapselt.
- Datensicherung erfolgt mit Offline Back-up oder mehrstufig digital und nicht überschreibbar, Wiederherstellungs-Tests sind etabliert.
- Es liegt ein Rechtekonzept vor mit einer Trennung in Administratoren und normale User, teilweise wird Zwei-Faktor-Authentifizierung verlangt.
- Gefordert ist eine Segmentierung der Systeme, insbesondere zwischen Produktion und Office, aber auch zwischen Standorten oder Funktionen (Drucker, Telefonie, ERP, HR).
- Ein Notfallplan und die Umsetzung von Schulungsmaßnahmen für die Mitarbeiter.

Tatsächlich muss das Thema IT-Sicherheit – auch unabhängig von einem tatsächlich eingetretenen Schaden – einen deutlich höheren Stellenwert einnehmen. Ähnlich wie in der Feuer-Versicherung trägt die Versicherungswirtschaft so (endlich auch) zur Verbesserung der Risikosituation bei den Kunden bei.

[1] https://www.tagesschau.de/wirtschaft/hackerangriffe-wirtschaft-unternehmen-corona-101.html

[2] https://www.psafe.com/blog/vazamento-expoe-numero-de-cpf-de-milhoes-de-brasileiros-alerta-psafe/

[3] https://www.bloomberg.com/profile/company/SNWL:US
und
https://www.sonicwall.com/de-de/

[4] https://www.bloomberg.com/news/articles/2021-01-23/cyber-firm-sonicwall-says-it-was-victim-of-sophisticated-hack

Dr. Sven Erichsen –
Erichsen GmbH

LITHIUM-IONEN-AKKUS: EIN BRANDRISIKO ETABLIERT SICH

Unser Alltag wird zusehends mobiler, und diese mobile Welt wird derzeit angetrieben von Lithium-Ionen-Akkus. Sie haben vor allem den Vorteil einer relativ hohen Energiedichte. Das ermöglicht kompakte Bauweisen und eine verhältnismäßig lange Nutzung vor dem nächsten Laden. Allerdings geht mit der Lithiumtechnologie ein Brandrisiko einher, wie sich mittlerweile herumgesprochen hat.

In den Statistiken des Institutes für Schadenverhütung und Schadenforschung (IFS) begannen Akkubrände vor gut zehn Jahren aufzufallen. Seither beobachten wir einen ebenso starken wie kontinuierlichen Anstieg der Fallzahlen. Diese Entwicklung führt das Institut in erster Linie auf die Verbreitung zurück, die in zwei Richtungen wächst: Fast jeder hat heute zum Beispiel ein Smartphone, viele sogar mehrere; und zugleich erobern Lithium-Ionen-Akkus eine immer breitere Produktpalette.

Waren es vor Jahren noch vor allem Notebooks und Smartphones, deren energiehungrige Displays mit effizienten Stromspeichern versorgt werden mussten, so lassen mittlerweile immer mehr Geräte die Netzleitungen hinter sich. Selbst Computermäuse sind teilweise mit Lithium-Ionen-Akkus ausgestattet, wie wir bei einer Brandursachenermittlung gelernt haben, und durch immer mehr Haushalte fahren Akkupacks per Staubsaugroboter spazieren.

Ein stark wachsendes Einsatzgebiet sind Elektro- und Mikromobilität. Hier treffen mit der benötigten starken Akkuleistung und den hohen betriebsüblichen Belastungen mehrere Risikofaktoren aufeinander. Außerdem gibt es produkttypische Risiken, zum Beispiel bei Hoverboards: Die Skateboards mit Elektromotor sind vor allem bei Jugendlichen beliebte Lifestyle-Produkte und werden zum Teil auffallend preisgünstig in Onlineshops angeboten. Das IFS hat schon mehrere Hoverboards untersucht, deren Akkus während des ersten Ladevorganges thermisch durchgegangen sind. Bei Rapex, dem Schnellwarnsystem der EU für Verbraucherschutz, gibt es eine lange Liste von Rückrufen. Produktqualität und Produktsicherheit gehen oft Hand in Hand.

Eine Erfolgsgeschichte schreibt das Elektrofahrrad. Mit 1,95 Millionen verkauften E-Bikes entschieden sich im vergangenen Jahr fast vier von zehn Fahrradkäufern für die Elektrovariante, meldet der Zweirad-Industrie-Verband. Doch das Dasein eines Drahtesels verlangt dem Akkupack manches ab, was die Lithiumtechnologie übel nimmt. Wenn das Rad samt Akku den Winter unbeachtet in der ungeheizten Garage fristet, können insbesondere bei den ersten Ladevorgängen der neuen Saison Defekte auftreten. Ein Defekt bedeutet in der Regel die explosionsartige Entladung der gespeicherten Energie. Auch Stürze können den Akku vorschädigen.

Weil ein Defekt bei Lithium-Ionen-Akkus eine erhebliche Brand- und Verletzungsgefahr bedeutet, ist es wichtig, die Risikofaktoren zu kennen und auf die richtige Handhabung zu achten. Die Herstellerangaben – insbesondere zur Eignung von Ladegeräten – müssen unbedingt beachtet werden, um Schäden zu vermeiden. Die häufigsten Fehlerquellen und die wichtigsten Sicherheitshinweise haben wir auf der IFS-Internetseite[1] zusammengefasst und um Videobeiträge ergänzt.

In der Brandursachenermittlung sind Akkus zu einem Standardkriterium geworden, das wie die Elektroinstallation bei jeder Untersuchung abgefragt und geprüft wird. Das Schadenpotential ist nach Ansicht des IFS nicht unverhältnismäßig hoch, doch es ist klar relevant.

[1] https://www.ifs-ev.org/schadenverhuetung/feuerschaeden/lithium-ionen-akkus/

Ina Schmiedeberg –
Pressereferentin IFS

Ein Hoverboard lädt inmitten brennbarer Gegenstände, als es im Akku zum Defekt und in der Folge zum Brandausbruch kommt.

Foto: IFS

TEAMS UND SHAREPOINT: INTERNE UNTERNEHMENS-KOMMUNIKATION 2.0

Die Art der Kommunikation innerhalb von Unternehmen hat sich von einfachen Wegen der Informationsübermittlung zu einem Netz aus verschiedenen digitalen Plattformen entwickelt, das einer Struktur bedarf.

Im Zuge der fortschreitenden Digitalisierung von Arbeitswelten und -prozessen stehen Mitarbeiter heutzutage immer mehr Informationen, jederzeit abrufbar, zur Verfügung. Verschiedenste Kommunikationskanäle und die Möglichkeit, mit einem Knopfdruck viele Menschen gleichzeitig zu erreichen, stellen Unternehmen zunehmend vor die Aufgabe, die Informationen für ihre Mitarbeiter auf direktem Wege gefiltert und aufbereitet zur Verfügung zu stellen.

Die Unternehmenskommunikation leistet einen bedeutenden Beitrag zur Zielerreichung und -umsetzung gewinnorientierter Unternehmen. Durch eine angemessene und innovative Kommunikationsstrategie des Leistungsangebotes und der Unternehmenskultur ist es möglich, sich von den Wettbewerbern zu differenzieren und Alleinstellungsmerkmale strategisch nach außen zu tragen. Um die strategischen Ziele zu erreichen, spielt die nach innen gerichtete Kommunikation eine entscheidende Rolle, sie bezieht jegliche interne Stakeholder-Gruppen mit ein und ist in der Art und Ausführung Bestandteil der Unternehmenskultur mit dem Ziel, den fachlichen und sozialen Austausch zwischen Mitarbeitern auch abteilungs- und hierachieübergreifend zu fördern.

Durch den Austausch hat die interne Unternehmenskommunikation zusätzlich einen entschiedenen Einfluss auf das Betriebsklima sowie die Motivation und Zufriedenheit der Mitarbeiter. Ausgehend von der Kommunikationsstrategie in dem jeweiligen Unternehmen müssen passende Kanäle und Tools etabliert und den Mitarbeitern zur Verfügung gestellt werden.

Klassische Medien für den Austausch werden in Unternehmen neben persönlichen Gesprächen häufig durch die Kommunikation per Telefon und E-Mail ergänzt. Bei der Umsetzung einer umfassenden Kommunikation, die den Austausch innerhalb von Organisationen mit einer Vielzahl an Standorten, Mitarbeitern, Abteilungen und Themenbereichen bildet, stoßen diese klassischen Kanäle vor allem bei der Praktikabilität jedoch an ihre Grenzen. Um die Anforderungen zu gewährleisten und dem Trend zu folgen, dass sich die allgemeine Kommunikation stetig auf eine Vielzahl an eingesetzten technischen Systemen erweitert, bietet ein auf das jeweilige Unternehmen ausgerichtetes Intranet / interne Kommunikationsplattform, wie zum Beispiel Microsoft Teams oder Slack, einen geeigneten Lösungsansatz.

Bei MARTENS & PRAHL setzen wir auf Microsoft Teams, um die verschiedenen Anforderungen optimal umzusetzen und sind mit dieser Lösung sehr zufrieden. Die Struktur von Microsoft Teams, die sich an beispielsweise Abteilungen und Arbeitskreisen ausrichten kann, fördert trotz der unterschiedlichen Arbeitsweisen an verschiedenen Standorten den Austausch untereinander zu gemeinsamen Projekten. Per Chat-Nachricht, Beitrag in einem Kanal oder integrierte (Video-)Telefonie-Option können Mitarbeiter miteinander kommunizieren, Themen platzieren und gemeinsam an Projekten arbeiten.

Zusätzlich zur Funktion als interne Austauschplattform, bietet die auf Sharepoint aufgebaute Ordnerstruktur eine Art Bibliothek zur Organisation themenbezogener Dateien und Dokumente.

So angenehm die Kommunikation durch die digitalen Medien geworden ist, so steigt stetig die Flut an Informationen, die über die zahlreichen Optionen, Anliegen loszuwerden und sich mitzuteilen, ankommen. Zwischen Nachrichten, E-Mails, Telefonaten, Blog-Beiträgen und persönlichen Gesprächen vor Ort können dabei relevante Informationen untergehen, wenn diese nicht an einem zentralen Ort gefiltert und aufbereitet zur Verfügung gestellt werden.

Eingebunden in Microsoft Teams bietet der Sharepoint mit der Einführung der Mini-Webseiten die Möglichkeit, diese Lücke bezüglich der Beständigkeit und des praktikablen Zugriffs auf relevante Mitteilungen zu schließen und die Informationsbeschaffung effizienter gestalten zu können. Dort können themenorganisiert relevante Informationen, Nachrichten und Dokumente aufbereitet und gefiltert dauerhaft zur Verfügung gestellt werden.

Diese digitale Lösung für die Kommunikation in Unternehmen bietet Möglichkeiten, die Inhalte in angemessener Form darzustellen. Durch die optische Aufbereitung und Strukturierung nach Themen können Informationen somit anwenderfreundlich gestaltet werden, um einen Mehrwert gegenüber der einfachen Vermittlung in Textform zu generieren. Durch die Struktur wird es den Mitarbeitern ermöglicht, alle nötigen Informationen auf einen Blick zu haben und sich einen Überblick zu verschaffen, wo sie schnell die von ihnen gesuchten Inhalte finden.

Die Aufbereitung der Beiträge als Artikel trägt zusätzlich dazu bei, dass Mitarbeiter auf kurzem Wege anhand von aussagekräftigen Headlines und Schlagworten entscheiden können, ob sie in die geteilte Information Zeit investieren wollen, oder ob ihnen durch die spezifischen Inhalte kein Mehrwert entsteht, um die ihnen zur Verfügung stehende Zeit effizienter einzuteilen und zu nutzen. Struktur und Optik wirken dabei nicht nur effizienzsteigernd, sondern können – bei gewähltem Einsatz der Corporate Identity bei der Gestaltung – die Marke des Unternehmens intern stärken.

Sowohl für bestehende Teams als auch für neue Kollegen bilden die Sharepoint-basierten Mini-Websites als Teil von Microsoft Teams einen Anlaufpunkt zur übersichtlichen Informationsbeschaffung und Einführung in Themenbereiche. Microsoft Teams bietet in Kombination mit dem Sharepoint einen erheblichen Mehrwert im Unternehmen.

Durch die stetig aufbereitete Weitergabe von fachlichem Wissen und der strukturierten Ablage projekt- und themenbezogener Dateien ist es auch im Zeitverlauf möglich, den Zugriff auf relevante Informationen für alle Mitarbeiter zu gewährleisten. Durch die einfache Art der Kommunikation, mit der alle Kollegen erreicht werden können, die den Bedarf an Informationen haben, und die effiziente Weitergabe von Inhalten kann somit die Kapazität von Teams für das Alltagsgeschäft sowie die projektbezogene Arbeit erhöht werden.

Anneke Witt –
MARTENS & PRAHL Holding

HAUSRATVERSICHERUNG

WENN WERTE SICH ENTWICKELN, MUSS DIE VERSICHERUNGSSUMME ANGEPASST WERDEN

Was ist über die Hausratversicherung versichert? Einfach gesagt ist alles versichert was rausfällt, wenn man das Haus bzw. die Wohnung auf den Kopf stellt. Hier sind Feinheiten wie Einbauschränke, Einbauküchen etc. zu berücksichtigen, da diese auch über die Wohngebäudeversicherung versichert werden können. Im Schadenfall wird der Wiederbeschaffungswert von Sachen gleicher Art und Güte in neuwertigem Zustand (Neuwertversicherung) ersetzt.

Die Versicherer bieten Tarife mit einer festen Versicherungssumme und einer Höchstentschädigung (Wohnflächentarif) an. Wichtig bei dem Erstgenannten ist, dass der Wert des Hausrates und die policierte Versicherungssumme (immer) übereinstimmen. In dieser Versicherungssumme müssen sich auch die Wertsachen wiederfinden. Für diese Übereinstimmung ist der Versicherungsnehmer verantwortlich. Denn auch wenn der Versicherer einen Unterversicherungsverzicht ausspricht, kann eine Unterversicherung, zum Beispiel durch Wertsteigerungen, eintreten. Bei Wohnflächentarifen ist bedingungsgemäß eine Höchstentschädigung festgelegt. Hierbei ist es wichtig, dass die Wohnfläche richtig ermittelt wird. Ist diese richtig ermittelt, leistet der Versicherer bis zur vereinbarten Versicherungssumme. Für Wertsachen gelten dann ebenfalls Höchstentschädigungen. Der Versicherungsnehmer hat also zu prüfen, ob die vereinbarte Entschädigungsgrenze für Wertsachen ausreicht und gegebenenfalls eine Anpassung vornehmen.

Im Schadenfall muss der Versicherungsnehmer den entstandenen Schaden gegenüber dem Versicherer nachweisen. In vielen Fällen ist es einfach, einen Wertnachweis zu erbringen. Beim Kauf teurer Werte ist die Empfehlung, den Kaufbeleg aufzubewahren und zusätzlich aussagekräftige Fotos zu machen. Sofern – wie zum Beispiel bei Erbstücken, Antiquitäten oder Kunstgegenständen – kein Kaufbeleg vorhanden ist, empfiehlt es sich, neben Fotos auch ein Gutachten durch einen Juwelier, Antiquitätenhändler oder Kunstexperten anfertigen zu lassen. Liegt kein Gutachten vor, wird es im Schadenfall schwer, einen Wertnachweis gegenüber dem Versicherer vorzuweisen. Ist dieser nicht möglich, wird der Versicherer im schlimmsten Fall nicht leisten.

Fazit: Jeder Hausrat ist anders und individuell ausgestattet. Die Versicherer bieten verschiedene Möglichkeiten, um dieser Individualität gerecht zu werden – auch in Hinblick auf die Wertsteigerungen. So haben einige Versicherer in ihren Bedingungen geregelt, dass Wertsteigerungen automatisch mitversichert sind, andere haben eine Vorsorgesumme vereinbart. Über unser Hausrat Premium Konzept mit der Allianz haben wir zum Beispiel eine 25 %ige Vorsorge und eine Vorsorge bei möglicher Wertsteigerung durch Tod des Künstlers.
Sprechen Sie daher Ihren Makler an, um die Versicherungssumme regelmäßig anzupassen.

Thomas Lindow –
MARTENS & PRAHL
Versicherungskontor GMBH, Hamburg

IMPRESSUM

Herausgeber:

MARTENS & PRAHL Versicherungskontor
GmbH & Co. KG
Moislinger Allee 9 c · 23558 Lübeck

Redaktion:

Chefredakteurin: Alexandra Jung

Autoren:
Dr. Sven Erichsen, Thomas Lindow, Julie Schellack,
Ina Schmiedeberg, Nikolaus Stapels, Anneke Witt

Kontakt:

E-Mail: holding@martens-prahl.de
Telefon: 0451 88 18 0

Konzeption, Realisation:

Gley Rissom Thieme & Co.
Agentur für Kommunikation Hamburg GmbH

Druckerei: VON DER SEE GmbH

Bildnachweis: Shutterstock, IFS

www.martens-prahl.de

grt-agentur.de

UNSERE BASIS FÜR DIE ZUKUNFT: WERTE UND WISSEN IN EINER FUNDIERTEN AUSBILDUNG

TRAMPOLIN/
DAS KARRIERE-PORTAL VON MARTENS/PRAHL/

Gut ausgebildete Mitarbeiter, die weiterdenken und unsere gelebten Werte in der täglichen Arbeit umsetzen, sind für uns die Basis nachhaltigen Erfolges.

Darum legen wir im Rahmen der Ausbildung bei MARTENS & PRAHL den Fokus auf genau diese Aspekte: Wir vermitteln fundierte Einblicke in das gesamte Versicherungswesen in Praxis und Theorie, setzen auf persönliches Coaching und die Teilnahme an Schulungen, Seminaren und überbetrieblichen Veranstaltungen in vielen Fachrichtungen, um die Ausbildung abwechslungsreich und spannend zu gestalten.

Alternativ zur klassischen Ausbildung bieten wir das duale Studium in den Fachrichtungen Betriebswirtschaftslehre oder Wirtschaftsinformatik an.

Willkommen auf unserem Karriere-Portal. Willkommen bei den besten Perspektiven für eine erfolgreiche Zukunft: www.trampolin-karriere.de

Hier geht's zum Karriere-Portal.

Moislinger Allee 9 c · 23558 Lübeck
T 0451 88 18 0 · F 0451 88 18 280

MARTENS/PRAHL/SICHER SEIN