IT-Sicherheit und Cloud-Management IV

Cyberangriff: Die arbeitsrechtlichen Folgen

Hackerangriffe können ganze IT-Systeme lahmlegen und ein Unternehmen faktisch handlungsunfähig machen, weil einfach nichts mehr geht. Aufträge sind da, die Mitarbeitenden auch, und trotzdem kann nicht gearbeitet werden. In einem solchen Fall müssen schnell die arbeitsrechtlichen Folgen geprüft werden.

› Brigitte Kraus-Meier

Längst ist bekannt, dass Hackerangriffe die IT-Struktur eines Unternehmens existenziell treffen. Trotzdem hört und liest man aber nicht viel über solche Schadensereignisse. Cyberangriffe können zu teilweisen oder gar vollständigen Betriebsausfällen führen. Und auch wenn der Zugang zum IT-System wiederhergestellt werden konnte, so bedeutet dies noch lange nicht, dass alle Daten wieder vorhanden sind und normal gearbeitet werden kann. Neben den hohen Anforderungen an das Krisenmanagement kommen Fragen hinzu, was man während eines IT-Shutdowns mit den Mitarbeitenden macht.

Arbeit nicht möglich

Führt ein Cyberangriff vorübergehend dazu, dass in weiten Teilen des Unternehmens gar nicht mehr gearbeitet werden kann, müssen die arbeitsrechtlichen Möglichkeiten schnell geprüft werden. Im Arbeitsrecht gilt der Grundsatz: Lohn wird für geleistete Arbeit bezahlt. Wird die Arbeitsleistung nicht erbracht, so erfolgt grundsätzlich keine Lohnzahlung, es sei denn, es liege ein Fall von unverschuldeter Arbeitsverhinderung des Arbeitnehmers vor oder ein Fall des Annahmeverzugs des Arbeitgebers.

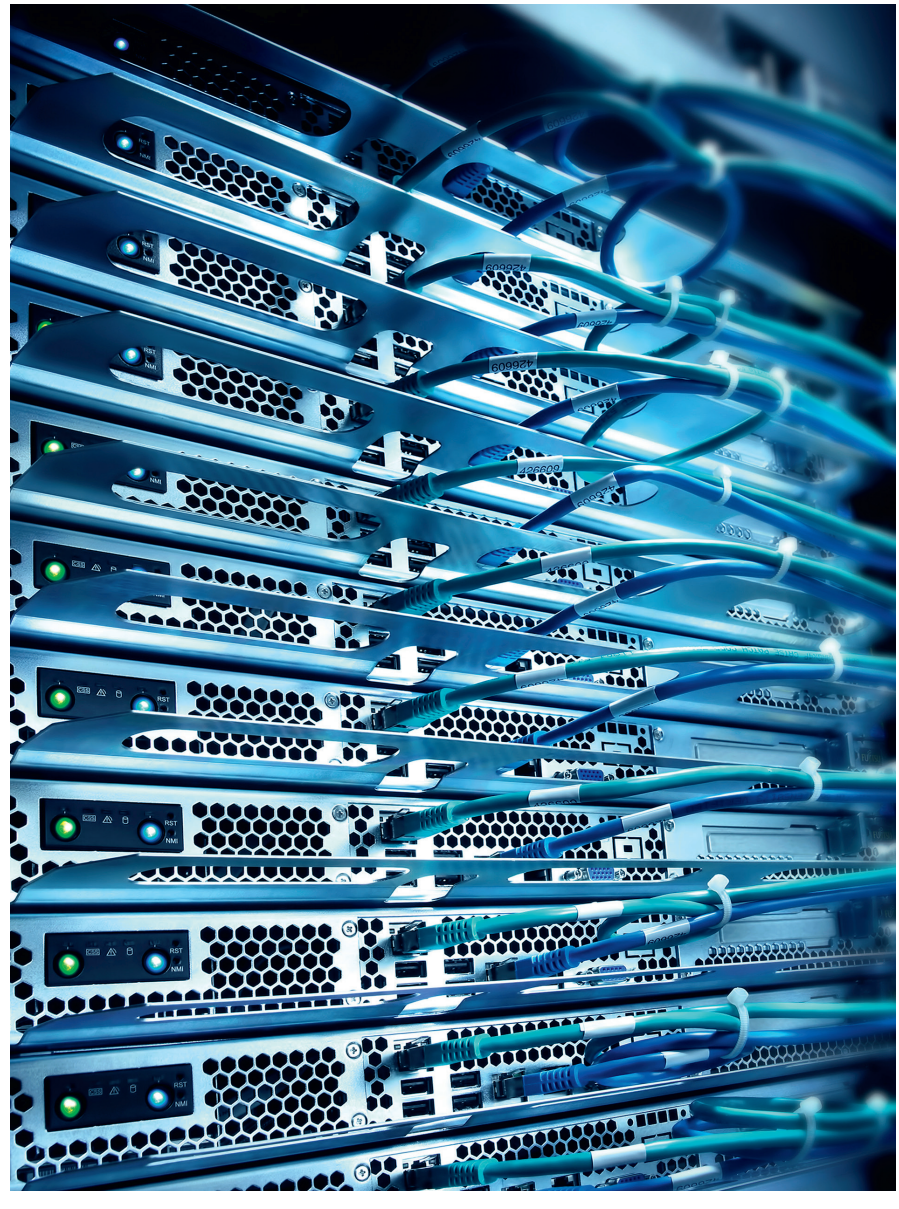
kurz & bündig

- Wird die Arbeitsleistung nicht erbracht, so erfolgt grundsätzlich keine Lohnzahlung, es sei denn, es liege ein Fall von unverschuldeter Arbeitsverhinderung des Arbeitnehmers vor oder ein Fall des Annahmeverzugs des Arbeitgebers.
- Selbst wenn ein Cyberangriff als Zufall oder höhere Gewalt gewertet wird, wäre wohl noch immer von einer Lohnzahlungspflicht auszugehen, da sich das Einzelereignis in der Risikosphäre des Arbeitgebers auswirkt.
- Unternehmen mit flexiblen Arbeitszeitmodellen sind in aller Regel im Vorteil. Die einfachste und schnellste Massnahme ist die Anordnung, dass Überstunden zu kompensieren sind.

So einfach die praxisrelevante Frage der Lohnzahlung scheinen mag, so komplex ist die juristische Unterscheidung. Liegt der Grund für die Arbeitsverhinderung in der Person des Arbeitnehmenden und ist diese vom Arbeitnehmenden unverschuldet, so gilt ein gesetzlicher Lohnanspruch gemäss Art. 324a OR. Bekannt ist dies bei Arbeitsunfähigkeit infolge Krankheit oder Unfalls. Cyberangriffe und die damit verbundene faktische Stilllegung des Betriebs stellen dagegen ein Risiko dar, das im Sphärenbereich des Arbeitgebers eintritt. Die Frage der Lohnzahlung, obwohl die Mitarbeitenden keine Arbeitsleistung erbringen, muss daher nach den Regeln des Annahmeverzugs des Arbeitgebers gemäss Art. 324 OR beurteilt werden. Dabei spielt es grundsätzlich keine Rolle, ob den Arbeitgeber für die Situation ein Verschulden trifft oder nicht.

Bei Hackerangriffen könnte allenfalls dann ein Verschulden vorliegen, wenn der Arbeitgeber überhaupt keine IT-Sicherungsmassnahmen ergriffen hat, das IT-System also sozusagen einen offenen Bereich darstellt. Die Realität zeigt aber ein anderes Bild. Unternehmen schützen ihre IT gewissenhaft, Hacker und Cyber-

Kriminelle finden aber dennoch immer wieder neue Schlupflöcher, um sich in betriebliche Systeme einzunisten. Selbst wenn ein Cyberangriff als Zufall oder höhere Gewalt gewertet wird, wäre wohl noch immer von einer Lohnzahlungspflicht auszugehen, da sich das Einzelereignis in der Risikosphäre des Arbeitgebers auswirkt.



Flexibilität gefordert

Unternehmen mit flexiblen Arbeitszeitmodellen sind in aller Regel im Vorteil. Die einfachste und schnellste Massnahme ist die Anordnung, dass Überstunden zu kompensieren sind. Diese Anordnung ist aber nur dann zulässig, wenn sich der Arbeitgeber vertraglich ausbedungen hat, dass er den Zeitpunkt der Überstundenkompensation bestimmen und damit die Kompensation anordnen darf. Viele Arbeitszeitreglemente machen aber genau vor diesem konsequenten Schritt halt und lassen zu, dass die Kompensation gemeinsam besprochen wird oder dass der Arbeitnehmende seine Kompensationswünsche eingibt. Nur dort, wo klar festgehalten ist, dass der Arbeitgeber einseitig den Zeitpunkt der Kompensation bestimmen darf, kann auch bei einem Cyberangriff kurzfristig die Kompensation von Überstunden verfügt werden. Der Umfang der Kompensation hängt natürlich vom Saldo der Überstunden ab.

Ob und wieweit Minusstunden angeordnet werden können, hängt wiederum von den bereits geltenden Anstellungsbedingungen ab. So ist beispielsweise denkbar, dass ein Jahresarbeitszeitmodell gilt, bei welchem sich die Schwankungen aufgrund betrieblicher Bedürfnisse ergeben und so auch möglich ist, dass die Mitarbeitenden zu Minusstunden verpflichtet werden. Wenn dies vertraglich sauber aufgestellt ist, so ist die Anordnung von Minusstunden denkbar. Allerdings muss den Mitarbeitenden die Möglichkeit geboten werden, die Minuszeit später wieder auszugleichen. Ist das nicht möglich und tritt beispielsweise ein Mitarbeitender im laufenden Jahr aus, so wäre ein Lohnabzug nicht gerechtfertigt, wenn der Grund für die Minuszeit ausschliesslich beim Arbeitgeber lag.

Eine weitere Möglichkeit besteht darin, dass der Arbeitgeber die Mitarbeitenden, welche nicht arbeiten können, nach Hause schickt, gleichzeitig von ihnen aber verlangt, dass sie auf Abruf sind und jederzeit wieder zur Arbeit aufgeboten werden können. Wenn der Arbeitgeber während dieser Zeit den Lohn voll bezahlt, kann er auch eine kurzfristige Verfügbarkeit verlangen. Der Mitarbeiter hat dann zwar nicht die Möglichkeit, die Zeit zu Hause frei zu gestalten, was aber gerechtfertigt ist. Mischformen sind ebenfalls denkbar, wenn diese zwischen Arbeitgeber und Arbeitnehmendem vereinbart werden.

Kurzfristige Ferienanordnung

Eine knifflige Frage ist jene der Ferienanordnung. Kann der Arbeitgeber aus betrieblichen Gründen kurzfristig Ferien anordnen, dies beispielsweise wenn durch den Cyberangriff die Arbeit schlichtweg nicht mehr möglich ist und die Mitarbeitenden gar nicht beschäftigt werden

können? Auch diese Frage wird kontrovers diskutiert. Zum einen gibt es die Haltung, der Ferienbezug könne nur mit einer Vorankündigung von drei Monaten angeordnet werden. Diese Regelung ist für den Sachverhalt eines Hackerangriffs aber völlig untauglich, denn die Arbeit kann jetzt nicht erledigt werden – Ferien in drei Monaten nützen dem Unternehmen nichts.

Die starre Anwendung der Ankündigungsfrist von mindestens drei Monaten ist nach Ansicht der Autorin nicht haltbar. Denn zum einen sieht das Arbeitsrecht klar vor, dass der Arbeitgeber den Zeitpunkt des Ferienbezugs bestimmt. Zum anderen gehen die betrieblichen Interessen vor, auf die Wünsche der Mitarbeitenden ist aber Rücksicht zu nehmen. Zumindest in jenen Fällen, bei denen ein Unternehmen infolge eines Cyberangriffs während längerer Zeit stillgelegt ist, dürfte denkbar sein, dass der Arbeitgeber mindestens einen Teil der Ferien zum Bezug anordnen darf.

Je älter der Feriensaldo ist, desto eher dürfen diese Ferientage angeordnet werden. Zu bedenken ist, dass Ferien nur dann als solche gelten, wenn der Erholungszweck gegeben ist. Wenn der Mitarbeitende über seine Zeit frei verfügen kann, ist das erfüllt. Muss er sich aber permanent bereithalten und weiss er nie, ob er morgen arbeiten muss, wird eine Erholung nicht gleich möglich und die Ferienanordnung unzulässig sein. Es zählt der Erholungszweck – nicht relevant sind die persönlichen Ferienpläne. Das Argument eines Mitarbeitenden, er könne nun nicht Ferien beziehen, weil er seine geliebte Feriendestination nicht erreichen könne, greift nicht.

Zeichnet sich ab, dass der Wiederaufbau der IT-Struktur wesentlich länger benötigt als ein paar Tage, sollte das Unternehmen die Anmeldung von Kurzarbeit prüfen. Die Frist zur Voranmeldung in wirtschaftlich «normalen» Zeiten von zehn Tagen führt aber meist dazu, dass diese Unterstützung wohl zu spät käme resp. das Unternehmen bis dann wohl schon wieder funktionsfähig ist.

Arbeit nachholen

Sind die IT-Systeme wieder hochgefahren und die Arbeitstätigkeit kann wieder ausgeübt werden, wird allenfalls das Leisten von Überstunden angeordnet oder nötig sein. Der Arbeitgeber darf dies selbstverständlich verlangen. Der Mitarbeitende muss Überstunden leisten, soweit ihm dies zumutbar ist und soweit die gesetzlichen Arbeits- und Ruhezeiten eingehalten sind. Ableitend aus der Treuepflicht des Arbeitnehmers könnte man weiter überlegen, dass allenfalls das Nacharbeiten entschädigungslos gefordert werden könnte.

Diese Meinung wird teilweise in der Lehre vertreten, wenn der Annahmeverzug nicht verschuldet, also insbesondere auf Zufall oder höhere Gewalt zurückgeht – wie dies bei einer Betriebsstilllegung nach einem Cyberangriff der Fall wäre. Leistet der Arbeitgeber den Lohn während der Stilllegung weiter, haben also die Mitarbeitenden keine Lohneinbusse, so wären nach Ansicht der Autorin die Mitarbeitenden zu einem gewissen Mass zur Nachleistung verpflichtet, ohne dass diese Stunden als Mehrstunden oder als zuschlagspflichtige Überstunden zu behandeln wären.

Regelungen prüfen

Die arbeitsrechtlichen Fragen bei einer Arbeitsverhinderung infolge eines Cyberangriffs sind jenen infolge des Coronavirus die gleichen, die Antworten aber nicht in allen Teilen. Kommt hinzu, dass während der Coronavirus-Pandemie das Instrument der Kurzarbeit ausgedehnt und ein neues hinsichtlich Erwerbsausfall-Entschädigung geschaffen wurde. Damit konnten die nicht klar geregelten arbeitsrechtlichen Konstellationen der Lohnzahlung – für die Dauer der Pandemie – umgangen werden, indem durch diese Instrumente Alternativen für die Lohnzahlung geschaffen wurden.

Arbeitgeber sollten die Lehren aus der Coronasituation und aus den wirtschaftlichen Folgen nach einem Cyberangriff ziehen und die Anstellungsreglemente einer dahingehenden Überprüfung unterziehen. «

Porträt

Brigitte Kraus-Meier
Inhaberin, Beraterin, Konzis

Brigitte Kraus, lic. iur., Executive Master CCM, ist Inhaberin von Konzis, der Agentur für Arbeitsrecht und Kommunikation in Zürich. Sie ist Juristin und Unternehmenskommunikatorin und begleitet Unternehmen in Veränderungssituationen, insbesondere bei Betriebsübernahme, Neuausrichtung, Personalmassnahmen sowie bei der Gesprächsführung und Verhandlung mit Gewerkschaften und Arbeitnehmervertretungen. Brigitte Kraus ist Partner für Arbeitsrecht und Kommunikation des Personalmanagement-Netzwerks hr4hr.ch.

Kontakt

info@konzis.ch
www.konzis.ch