VOR DIE LAGE KOMMEN

oder

Wie kommen wir dazu, dass **wir** die Krise managen und nicht **sie uns**!

(Frei nach einer tatsächlichen Begebenheit – von Robert Bauer)

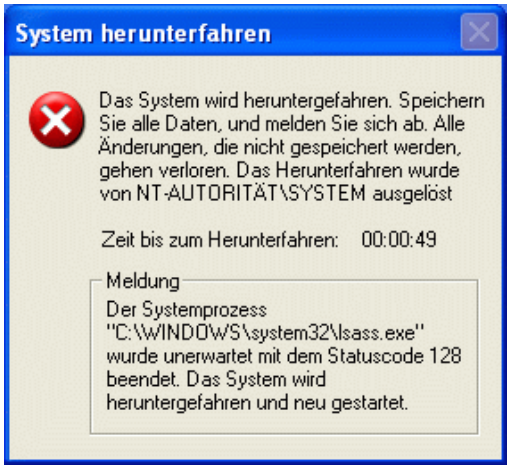
Eigentlich sollte es ja ein ganz normaler, eher ruhiger Arbeitstag werden. Vielleicht ergibt sich ja sogar die Möglichkeit, einigermaßen pünktlich aus der Arbeit weg zu kommen, um sich dann noch mit ein paar Freuden im Biergarten zu treffen. Das klingt doch ganz gut – oder?

Um 11 Uhr vormittags dann ein Anruf von der IT Hotline. Sie haben jetzt vermehrt Anrufe von Anwendern die beklagten, dass sich ihr PC ganz sonderbar verhält. Ein Blick auf die Auslastungsstatistik der Hotline: In der Tat, ca. 20 Anrufer in der Warteschleife – etwas viel für diese Tageszeit. Die Hotline wäre eigentlich gut besetzt, aber alle sind gerade am Telefon. Ich ruf nochmals an und frage was da los ist – nein, nicht aus Neugier, sondern weil es mein Job ist.

Ich bin einer der drei IT-Krisenmanager bei uns in der Firma – ein weltweit agierendes DAX-Unternehmen - und für den reibungslosen Betrieb von 65.000 Endgeräten zuständig. Drei Krisenmanager deshalb, weil wir im Falle einer IT-Krise den Vorsitz des Krisenstabes übernehmen und der tagt, so lange die Krise dauert, rund um die Uhr – also 3 Schichten.

Noch bevor ich jemand von der Hotline sprechen kann, kommt ein Kollege vom Netzwerkbetrieb bei mir am Schreibtisch vorbei. „Du, wir haben sehr hohe Netzaktivitäten und können uns das nicht erklären!“ Jetzt sind schon 80 Anrufer in der Warteschleife – verdammter Mist, da braut sich was zusammen. Bei uns im Büro verhalten sich die Computer noch normal – noch!

Endlich mehr Infos von der Hotline. Auf den PCs erschein ein Fenster mit der Nachricht, dass das Gerät in 5 Sekunden runtergefahren wird und alle geänderten Daten verloren sind. Das passiert dann auch. Anschließend wird der PC wieder automatisch gestartet, aber er lässt sich nicht mehr bedienen. Er tut gar nichts mehr – zumindest im Vordergrund, aber im Verborgen läuft da viel, wie wir später erfahren sollten.



Jetzt schon 120 Anrufer in der Warteschleife. Wir schalten den Anrufbeantworter und eine Sondermeldung im Intranet ein. Ich nehme gleich mal Kontakt zu unseren Virenschutz-Spezialisten auf und erreiche sie gerade noch, bevor sie zum Mittagessen gehen.

Diese rufen sofort bei Heise an, sowas wie das RKI für Computerviren. Von dort wird bestätigt, dass seit heute Morgen verstärkt und rasant ausbreitend ein neuartiger Virus beobachtet wird. Die Netzwerker sind sehr besorgt! Der Traffic steigt enorm – und das weltweit. Erste Hiobsbotschaft aus der Produktion. Ein Lagersystem ist ausgefallen. Die Montage kann nicht mehr mit Teilen versorgt werden.

Ich telefoniere mit dem anderen Krisenmanager und den Virenschutzleuten und Netzwerkern, Krise ja/nein und Sofortmaßnahmen ja/nein. Als amtierender Krisenmanager on Duty liegt die Entscheidung bei mir. Schlagartig kommt mir eine Handlungsmaxime aus meiner Bundeswehrzeit in den Kopf: „Wenn schon Sch …, dann mit Schwung"!

Wir rufen ab sofort die IT-Krise aus. Der Krisenstab wird alarmiert und muss sich innerhalb von 30 Minuten im Krisenraum einfinden. Parallel dazu machen wir alle Netzwerke dicht, schließen Gateways und Firewalls und unterbinden jeglichen Datenverkehr über interne Netze und ins Internet. Wir verhängen quasi eine häusliche Quarantäne für alle und beschließen eine absolute Ausgangssperre. Ich informiere – wohlgemerkt informiere – den CIO über den sofort gültigen Krisenmodus. Damit werden alle gängigen Hierarchien und Anweisungswege außer Kraft gesetzt und der Krisenstab hat das alleinige Sagen.

Schön langsam trudeln die Mitglieder des Krisenstabs im Krisenraum ein. Jede Position ist wie gesagt mindestens dreimal besetzt, im Schnitt sind beim ersten Meeting 2 davon anwesend. Neben den IT-Spezialisten gibt es einen Schriftführer, der die Lage visualisiert und alle Entscheidungen mit Uhrzeit dokumentiert. Außerdem ist jemand für die Kommunikation zuständig.

Das erste Meeting stellt als erstes die Lage fest. Was ist alles betroffen, was wissen wir bereits über das Virus, wie verbreitet es sich, gibt es gewisse Muster bei den Infektionen quasi besonders vulnerable Gruppen, sind alle Regionen gleichermaßen betroffen oder gibt es lokale Hotspots, ist schon eine Reaktion nach dem Shutdown der Computernetze erkennbar, …. Alles wird fein säuberlich dokumentiert.

Wichtig für die Arbeit im Krisenstab, es werden Fakten berichtet, die dann unkommentiert zur Kenntnis genommen werden und zum Lagebild beitragen. Jedes Kommentieren oder „man müsste" ist in dieser Phase kontraproduktiv und muss vom Leiter unterbunden werden. Ausgehen von der ersten Lageübersicht werden dann die Aufträge an die einzelnen Spezialisten für weiter Recherchen zur Lage erteilt. Nach ca. 15 Minuten geht man auseinander, und jeder Spezialist versucht für sich und mit Hilfe seiner Kollegen am Arbeitsplatz weitere Fakten zu sammeln. Der Krisenstab trifft sich dann wieder zur nächsten vollen Stunde, und in diesem Stunden-Zyklus geht es nun weiter.

Zuvor wurde noch kurz die Schichteinteilung festgelegt. Schichtwechsel soll um 22 Uhr sein. Die Mitglieder der Nachschicht werden ab sofort nach Hause geschickt um zu schlafen oder sich zumindest zu erholen, dass sie dann fit für die Nachtschicht sind.

Noch eine halbe Stunde bis zum nächsten Termin. Endlich mal Zeit um selbst etwas runter zu kommen. Mit Mittagessen wird's wohl nichts, aber ich hole mir ein belegtes Baguette aus der Kantine. Gleichzeitig bestelle ich Getränke, Kaffee und Häppchen für den Krisenraum. „Ohne Mampf kein Kampf" – aber das war schon wieder Bundeswehr.

Gleichzeitig aber kommen jetzt andere Gendanken in mir hoch. „Verdammt nochmal, du hast ja für das was du jetzt machst, eine Ausbildung genossen". Jährlich einmal 3 Tage Ausbildung zum Krisenmanagement und zusätzlich zwei ganztägige Krisenübungen. Dies und den Nachweis dafür verlangt sogar die BaFin bei der jährlichen Bilanzprüfung.

Jetzt kommt er hoch in meinem Kopf, ich spüre es ganz genau. Er lässt sich nicht aufhalten und hämmert auf mein Hirn – der Satz, den uns unser Krisenstabstrainer immer und immer wieder einbläute: „DU MUSST SO SCHNELL WIE MÖGLICH VOR DIE LAGE KOMMEN!"

Ha – leichter gesagt als getan! Was heißt das denn, „vor die Lage"! Ich kann doch dem Virus nicht sagen, was er tun soll! Nein – aber du musst das Virus besser durchschauen. Du musst wissen wie er funktioniert, wie er sich verbreitet, wie man ihn eindämmen kann und vor allem darfst du dich nicht von ihm überraschen lassen. Er muss für dich berechenbar werden und du musst für jede seiner Aktionen sofort eine passende Reaktion parat haben. Du musst dabei auch Szenarien durchdenken, die zunächst ziemlich unmöglich erscheinen. Das Virus kann plötzlich in Mutationen auftreten und dies darf nicht wie eine komplett neue Welle wirken. Also lass uns Speed aufnehmen um zu überholen. Und wenn wir dann mal vorne sind, lassen wir uns das nicht wieder nehmen (auch wenn scheinbar Ruhe in der Sommerpause ist).

Der wichtigste Input für die nächsten Lagebesprechungen kam von unseren Spezialisten vom Virenschutz, also den Virologen, die sich dabei eng mit Heise (dem Computer RKI) abgestimmt haben. Zunächst die schlechte Nachricht, sie sind noch dabei das Virus zu sequenzieren, also die Computerprogramm-fitzelchen zu analysieren auf ihren „Verbreitungscode" und den „Schadsoftwareteil". Es gibt zurzeit weder Software zur Beseitigung des Virenprogrammes (also ein Medikament) noch einen Virenschutz der die Übertragung und Einnistung im Betriebssystem verhindert (als einen Impfstoff).

Die gute Nachricht – es scheinen nur Windows Systeme betroffen zu werden (also Menschen). Andere Populationen wie UNIX, IOS etc. (also Tiere – Apple möge mir verzeihen) werden nicht befallen und verbreiten das Virus auch nicht. Zudem erfolgt die Weitergabe ausschließlich über direkte Netzwerkkontakte – also Maschine zu Maschine (Mensch zu Mensch) – und nicht über Dateien oder EMails (keine Schmierinfektion).

Ergeben sich da Chancen – fragt mich das einfach nicht mehr weggehende kräftige pochen in meinem Kopf mit der penetrant vorgetragenen Botschaft - VOR DIE LAGE – VOR DIE LAGE – VOR DIE LAGE - …

Trotzdem, die Krise wird länger dauern. Unser Teammitglied für Kommunikation wird beauftragt, dies im Unternehmen zu kommunizieren. Das heiß auch, dass wir die Mitarbeiter in der Fertigung, die bis jetzt in der verlängerten Mittagspause waren, nach Hause schicken können. Mit dieser Schicht, und vermutlich auch mit der nächsten, wird es wohl nichts mehr.

Schock! Mitten in der Bestandsaufnahme zu einem Lageupdate ging im Krisenraum plötzlich die Tür auf, und der CIO (oberster IT Chef) betrat den Raum. Es wurde mucksmäuschenstill. „Lasst Euch durch mich nicht stören, ich will nur zuhören" meinte er beschwichtigend. Doch! Du störst – und zwar ganz gewaltig. Eigentlich für die Krisenstabsarbeit ein absolutes „No Go" wenn hier die Hierarchie dazwischen funkt. Die Spezialisten müssen im angstfreien Raum ungestört alles vorschlagen können, ohne an ihre nächste Beurteilung zu denken. Noch schlimmer, wenn dann auch plötzlich noch Vorschläge, die eigentlich als Anweisungen empfunden werden, dazwischenfunken. Gemeinsam schafften wir es ihn davon zu überzeugen, dass seine Anwesenheit kontraproduktiv ist. Im Gegenzug dazu musste ich ihm zusagen, dass er fortan nach jeder Sitzung kurz mündlich oder telefonisch auf dem Laufenden gehalten wird.

Bei einem der Gespräche klagt er mir sein persönliches Leid. Er, nennen wir ihn Jens, wird enorm von den Werksleitern weltweit (nennen wir sie Ministerpräsidenten) bedrängt, weil sie ihre Produktionszahlen nicht erreichen können, da wieder einmal „die IT spinnt". Dies schlägt sich nachteilig auf ihre Reputation (sprich Wahlergebnis) nieder. Zudem sitzt ihm der CEO (nennen wir sie Angela) im Nacken.

Und da war es schon wieder – VOR DIE LAGE!

Na gut, dann lass uns doch mal was versuchen. Wir lassen die UNIX Server wieder ans Netz gehen und damit auch die Mailsysteme die mit diesen Servern arbeiten. Aber nicht gleich weltweit, sondern erst mal in einem begrenzten Gebiet. Der Krisenstab entschied sich für Südafrika – nicht, weil uns das weniger wert ist, sondern weil wir dort mehr Virenspezialisten sitzen haben, als sonst wo auf der Welt und außerdem liegt es in der gleichen Zeitzone. Irgendwie hab ich das Gefühl, wir setzen jetzt zum Überholen an.

Gibt es eigentlich von Heise schon was Neues? Ja – sie haben die ausführbaren Programmteile gefunden, die sich im Betriebssystem einnisten. Dort kopiert sich die Software und wird bei nächsten Netzwerkkontakt quasi wie ein Broadcast an alle erreichbaren, am Netz hängenden Computer geschickt! Das ist ein dreistelliger R-Wert und die Inkubation dauert Millisekunden!

Betrifft das auch Rechner mit den letzten, aktuellen Sicherheitsupdates? Ja leider. Die Schwachstell war zwar bei Microsoft seit kurzem bekannt, ist aber noch nicht geschlossen worden.

Inzwischen erfahren wir außerdem von Heise, dass auch so gut wie alle anderen Firmen betroffen sind. Siemens hat es schwer erwischt, aber auch die Deutsche Bahn (seit wann ist die so hoch digitalisiert?). Naturgemäß gibt es lokal dort viele Infektionen, wo die Rechner über ein Corporate Network eng zusammen sind – also in Firmen (Bars, Kneipen). Einzelpersonen an ihren PC's zu Hause sind weniger betroffen, da ihre Kommunikation im Wesentlichen über EMails stattfindet. Auch PC-Schulungsräume (Schulen, Kindergärten) sind nicht so arg betroffen, warum wissen wir aber allerdings noch nicht.

Gerüchtemäßig soll ein Cyber-Event in Ischgl maßgeblich zur Verbreitung beigetragen haben.

Der Test in Südafrika verlief erfolgreich. Trotz der gezielten Öffnung mit den Hygienemaßnahmen keine Neuinfektionen – juhu, wir sind auf der Überholspur!

Jetzt können wir diese Strategie weltweit ausrollen. Aber bitte trotzdem immer alles schön monitoren (testen – testen – testen).

Jetzt erweist es sich als sehr hilfreich, dass wir schon vor Jahren für diese Situation Notfallpläne entwickelt haben. Die Produktionsdaten für die Werke, die sonst online übertragen werden, zerhacken wir in verkraftbare Dateigrößen und verschicken sie per EMail. Im Werk werden die Dateien dann wieder zusammengesetzt und damit kann die Produktion notdürftig weitergehen. Und dann gab es da auch noch diesen findigen Meister in der Fertigung, der einen Stapel alter Papierformulare für den Notfall aufbewahrt hatte. Anstelle die Daten jetzt in den Computer einzugeben, hat er wie früher die Formulare ausgefüllt, die dann später problemlos nacherfasst werden konnten. Kleine Helden gibt es eben überall!

Mehr können wir jetzt im Moment nicht tun, als auf diejenigen zu warten, die jetzt fiberhaft auf der Suche nach Gegenmittel sind. Microsoft, das für Windows einen Patch (Impfstoff) erstellen muss, um die Sicherheitslücke zu schließen und Symantec, Norton oder wie sie alle heißen, die zusätzlich ihren Virenschutz updaten müssen und für die Beseitigung des Virus auf bereits infizierten Geräten (Medikament) sorgen.

Und ich warte jetzt auf meine letzte Sitzung des Krisenstabs um 22 Uhr um an meinen Kollegen zu übergeben. Eigentlich bin ich ziemlich fertig und gerädert. Wie schön wäre es doch im Biergarten gewesen, aber jetzt mag ich nur noch nach Hause und ins Bett. Morgen um 6 Uhr muss ich wieder antreten.

Am nächsten Tag war ich schon um Viertel vor 6 im Krisenraum. Berufsverkehr vor 6 Uhr sieht halt anders aus, als nach 7 Uhr. Ich genehmigte mir noch eine Tasse lauwarmen Kaffee vom Vortag – aus der Thermoskanne – sei's drum. Eigentlich sollte ja unser dritter Kollege diese Schicht fahren, aber der ist gerade in Urlaub und wir haben uns dazu entschieden, ihn nicht zurück zu holen – gnadenlos optimistisch eben.

Ich betrachtete die Lage-Mitschriften auf den Flip Charts aus der Nacht. Scheint nichts Außergewöhnliches passiert zu sein und offensichtlich sind wir immer noch VOR DER LAGE – ja, da war es schon wieder!

Um 6 Uhr dann gemeinsame Lagebesprechung mit alter und neuer Schicht. Microsoft hat in der Nacht mitgeteilt, dass sie den Patsch zum schließen der Sicherheitslücke im Laufe des Tages liefern können – Yippie, wir bekommen einen Impfstoff. Symantec und Norton haben ihre Software (Medikamente und Desinfektionssoftware) für den späten Nachmittag angekündigt. Blöd das, denn eigentlich bräuchten wir die zuerst. Aber immerhin, alles heute!

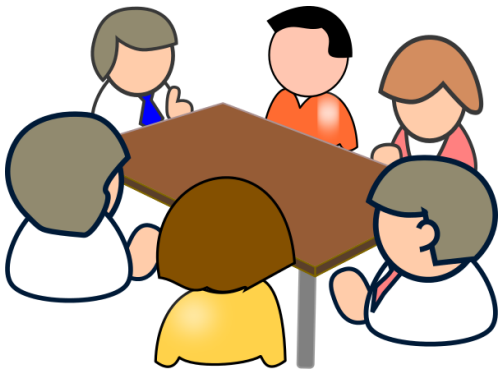
Über Nacht gab es kaum Neuinfektionen. Die wenigen, die wir durch Testen messen konnten, waren leicht in ihrer Infektionskette nachzuvollziehen. Ja – wir sind noch VOR DER LAGE! Trotzdem kein Grund zur Beruhigung. Nachdem das Teil sich so wahnsinnig schnell vermehrt, müssen wir bei den nächsten Schritten äußerst kontrolliert und behutsam vorgehen.

Wir haben jetzt noch ca. 8 Stunden Zeit, bis Impfstoff und Medikament da sind – Zeit die wir für eine ausgeklügelte und sichere Rolloutplanung (Beseitigen und Impfen) nutzen müssen. Die Krisenstabsarbeit sollte jetzt in einen Brainstorming-Modus wechseln.

Wir entschieden uns zunächst nochmals die aktuellsten Daten für den nächsten Lagebericht um 7 Uhr zu sammeln. Dann aber soll es, sofern sich daraus keine dramatische Situation ergibt, in Arbeitsgruppen weiter gehen. Und so war es dann auch:

Wir bildeten um 7 Uhr 3 Arbeitsgruppen, in welchen nicht nur die Mitglieder des Krisenstabs waren, sondern auch weitere Spezialisten aus den Fachbereichen hinzugezogen wurden – es war ja auch schon normale Arbeitszeit.

Die erste Arbeitsgruppe kümmerte sich darum zu planen, wie wir mit Hilfe der erwarteten Software der Virenschutzhersteller die infizierten Windows-Systeme (Server und PC's) vom Virus befreien können. Hinzu kommt der Untersuchungsauftrag, wie sich die so gereinigten Geräte verhalten werden und ob es Folgeschäden gibt.



Die zweite Gruppe sollte sich mit der Rollout Strategie für den Microsoft Sicherheitsupdate kümmern. Es ist sicher nicht möglich, alle 65.000 PC's und 5.000 Server zu Fuß zu besuchen und das Update per CD einzuspielen. Wir haben aber schon seit Jahren die Möglichkeit der Verteilung über das Netzwerk. Dazu müssen wir aber das Gerät wieder ans Netz hängen und wie stellen wir dabei sicher, dass dieser Patch auf den Geräten ankommt, bevor das Virus da ist? Außerdem können wir nicht alle Geräte übers Netz erreichen. Einige sind ausgeschaltet und werden vielleicht erst in ein paar Tagen wieder eingeschaltet, wenn der Mitarbeiter aus dem Urlaub kommt.

Andere Geräte haben wir zwar in der Liste, sind aber vom Netz getrennt und stehen irgendwo auf dem Schrank, weil sie im Moment nicht benötigt werden. Üblicher Weise kann man über das Netzwerk am ersten Tag so 70% bis 80% der Maschinen erreichen – wenn's gut geht.

Und eine dritte Gruppe hatte den wahrscheinlich wichtigsten Job. Sie sollten Maßnahmen erarbeiten, wie wir trotz weiterhin vorhandener Infektionen das Netz in Betrieb nehmen können, ohne dass eine weitere Welle über uns hereinbricht. Auf gut Deutsch – wie können wir mit dem Virus leben.

Um 13 Uhr stellten die Gruppen ihre Ergebnisse vor. Naturgemäß dauerte diese Session jetzt etwas länger aber ich hatte das gute Gefühl, dass wir einen tragbaren Plan haben. Die Teams gönnten sich eine ausführliche Kaffeepause – haben sie sich auch verdient. Ich informierte den CIO und gleichzeitig bereitete unser Kommunikationsspezialist die Information an alle Mitarbeiter vor. Als DAX Unternehmen mussten wir natürlich auch die Aktionäre und die Öffentlichkeit informieren – aber dies machte diesmal dann ausnahmsweise die standardmäßig dafür zuständige Konzernkommunikation.

Mein Kopfgeräusch änderte seinen Tonfall. „Ihr seid ja immer noch VOR DER LAGE und ihr habt einen Plan! Sieht gut aus!"

Am späten Nachmittag bekamen wir dann fast zeitgleich die Virenschutzprogramme sowie den Sicherheitsupdate von Microsoft. Aber jetzt nur nicht fahrlässig werden! Wie immer, wenn wir neue Updates bekommen, testen wir diese erst in der Laborumgebung auf Verträglichkeit mit unseren Installationen. Da heißt, wir führten erst unsere eigenen Testreihen mit dem neuen Impfstoff durch. Nach ca. 5 Stunden bekamen wir dann das i.O. von unseren Windows- und Virenspezialisten. Der Rollout konnte beginnen.

Gut, dass es jetzt schon wieder spät am Abend war, und ein Großteil der Geräte ausgeschaltet. Dies half uns, dass beim „Drücken des Startknopfes" nicht sofort eine heillose Überlastung des Unternehmensnetzwerks drohte. Dass der Rollout beim Einschalten der Geräte so funktionierte, dass das Virus gegenüber dem Sicherheitsupdate keine Chance hatte, hatten wir im Labor getestet und zig-fach erprobt.

Am nächsten Vormittag, den Tag 3 der Krise, konnten wir feststellen, dass ein Großteil der Computer jetzt sicher geschützt war. Der Virenschutz in den Netzservern und Firewalls sorgte dafür, dass es kaum mehr Verbreitungsmöglichkeiten gab. Der Sicherheitsupdate von Microsoft war auf fast 80% der Geräten eingespielt, sie waren also erfolgreich geimpft. Die wenigen noch infizierten Geräte sahen wir im Netzwerk und konnten gezielt dagegen angehen – ja, es bleiben halt immer Restarbeiten übrig. Für dies aber benötigte es keine Krisenorganisation mehr, sondern diese konnten von der Linie erledigt werden.

Um 11 Uhr dann konnten wir die Krise auch formal beenden – aber halt, ein wichtiges Teil fehl uns noch.

Gleich für den Nachmittag verabredeten wir uns zu einem „lessons learned" – Meeting. Ganz wichtig und zwar so lange die Eindrücke noch frisch sind. Mit diesen Erkenntnissen aus den „lessons learned" marschierten wir zu unserem CIO – wir, die Leiter Krisenstab sowie die Chefs der betroffenen Fachabteilungen.

Ergebnis: Wir bekamen 3 Projekte genehmigt um zu verhindern, dass uns so etwas noch einmal passiert und wenn es passiert, dass es glimpflicher abläuft.

In der Folge gab es noch mehrere gefährliche Computer-Vieren, die uns aber entweder gar nicht getroffen haben oder deren Abwehr uns ohne 3 Tage Krisenmodus gelang.

Sicher ist ein Computer-Virus etwas ganz anderes als ein menschlicher Virus und Sasser ist nicht vergleichbar mit Covid-19 – aber um das geht es gar nicht!

Es geht vielmehr um die Frage eines **erfolgreichen Krisenmanagements**. Wir können oft mal aus ganz anderen Disziplinen über Analogien lernen. Warum tun wir es denn dann nicht! **Und plötzlich ist das Hämmern in meinem Kopf wieder da! Sie wissen schon, VOR DIE LAGE KOMMEN!**