[Anm. des Managments: Dieses Dokument enthält sensibele Informationen und wurde nur aus Gründen der Transparenz geschwärzt offengelegt. Betroffen waren nur interne Client-Systeme, nicht der Endbenutzer.]

Sehr geehrte [redacted],

bereits seit einigen Tagen kam es bei unserem Server zu ungewöhnlich [redacted]

Deswegen schlug unser IT-Management vor, in Form neuer Server und neuer Hardware aufzurüsten. [redacted]

Heute gegen 13:25 Uhr konnte einer unsere Mitarbeiter der Security-Abteilung unzulässig [redacted] feststellen. Der Vorgang wurde bereits am Vormittag beobachtet, wie wir in den sofort eingeleiteten Untersuchungen herausfanden, durch einen Fehler in der Befehlskette und [redacted] wurde dieser aber [redacted] als unwichtig klassifiziert.

Wir ergriffen sofort weitreichende Maßnahmen, um diesen Fehler zu exekutieren und die negative Tragweite zu minimieren, was uns [redacted] nach einem geraumen Zeitraum gelang.

So war es uns nach einigen Stunden intensivster Arbeit mit allen Ressourcen [redacted], das Problem zu finden.

Nach knapp 2 Stunden war es möglich, das Problem zu finden um im Laufe des Tages wurde die Ursache sowie ihre Folgen immer klarer.

[Anm. des Managments: Dieses Dokument enthält sensibele Informationen und wurde nur aus Gründen der Transparenz geschwärzt offengelegt. Betroffen waren nur interne Client-Systeme, nicht der Endbenutzer.]

Rückblickend konnte folgender Tathergang von unseren Forensikern rekonstruiert werden und es hat sich folgendes ereignet:

[Vor 23:58 -> Ermittlungen laufen] hat [redacted]

Diese Aktivität zog sich lückenhaft bis um 7:45 Uhr.

Im Laufe des Vormittages wurden erste Anzeichen von uns identifiziert, konnten aber aufgrund verschiedener unternehmens-interner Umstände nicht behoben werden.

Um 13:25 wurde das Problem von einem unserer Experten klassifiziert und wir starteten weitreichende Schritte.

Im Laufe des Nachmittages wurde durch Grundlagenforschung verschiedene Ereignisse bekannt:

- das [redacted] Backup vom 05.03.2024 um 10:57 Uhr war vollständig vorhanden und funktionstüchtig
- der [redacted] zuletzt aktiv [redacted]

Um 16:15 wurde die Wiederherstellung [redacted]

Um 16:30 wurde mit dieser Schadensaufstellung begonnen und die Marketingabteilung beauftragt, ein Rundschreiben an alle betroffenen Personen zu verfassen.

17:00 Uhr: Das Problem wird zurückdatiert auf mindestens 00:46 Uhr

17:33 – jetzt Die Wiederherstellung der über [redacted] mit [redacted] befindet sich im vollen Gange und wird dauerhaft überwacht.

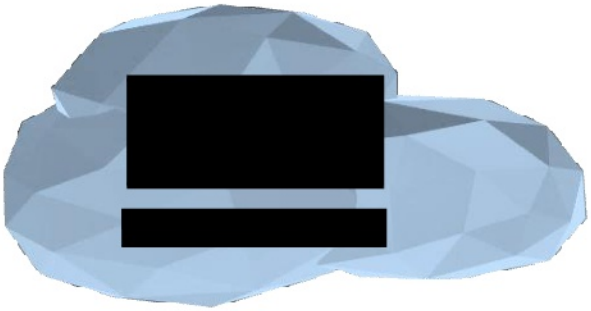
[Anm. des Managments: Dieses Dokument enthält sensibele Informationen und wurde nur aus Gründen der Transparenz geschwärzt offengelegt. Betroffen waren nur interne Client-Systeme, nicht der Endbenutzer.]

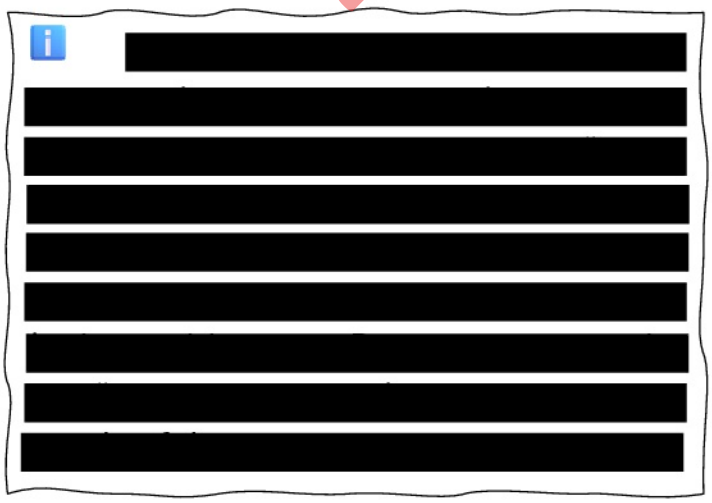
Unsere präventiven Maßnahmen, um Probleme vorzubeugen:

[redacted]Server des branchenweit führendend Dienstes Cloudflare, um die Quell-IP-Adresse zu schützen.

[redacted]

Um zukünftig solche Probleme zu vermeiden hat unseren Krisenstab beschlossen, eine Änderung der Zugriffstruktur zu instruieren. Nach [redacted]





Diese Pressemitteilung wurde in Zusammenarbeit von Marketing, Management und IT erstellt.

Weitere Anfragen richten Sie bitte an unsere Pressesprecherin oder an server@schächner.de.