

Sehr geehrte Nutzer und Investoren,

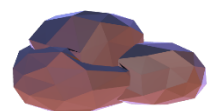
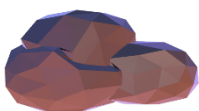
bereits seit einigen Tagen kam es bei unserem Server zu ungewöhnlich erhöhten Lastspitzen, die auch die von uns speziell hinzugezogenen Experten nicht wirklich erklären konnten. Deswegen schlug unser IT-Management vor, in Form neuer Server und neuer Hardware aufzurüsten. Wir begrüßen diesen Schritt sehr und ermuntern auch Sie, uns dabei zu unterstützen. Gerechtfertigt wird diese Maßnahme unter anderem durch den erhöhten Mehraufwand, der im Laufe der Tage (dadurch) entstand.

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

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

So war es uns nach einigen Stunden intensivster Arbeit mit allen Ressourcen daran nicht möglich, 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.



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

[Vor 23:58 -> Ermittlungen laufen] hat der Benutzer „Josef Schächner“ damit angefangen, Dateien aus dem externen Speicher „Fotosharing“ zu löschen.

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

Im Laufe des Vormittages wurden erste Anzeichen von uns identifiziert, konnten aber aufgrund verschiedener unternehmensinterner 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:

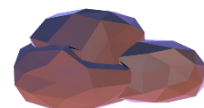
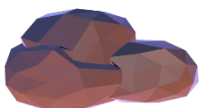
- das inkrementelle Backup vom 05.03.2024 um 10:57 Uhr war vollständig vorhanden und funktionstüchtig
- der Benutzer Josef Schächner hatte sich zuletzt aktiv angemeldet

Um 16:15 wurde die Wiederherstellung der Fotos aus dem Papierkorb des Benutzers Josef Schächner gestartet.

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 220 GB mit 4000 Dateien befindet sich im vollen Gange und wird dauerhaft überwacht.



Unsere präventiven Maßnahmen, um Probleme vorzubeugen:

Entgegen erster Gedanken leiten wir den Traffic der SchächnerCloud über amerikanische Server des branchenweit führenden Dienstes Cloudflare, um die Quell-IP-Adresse zu schützen.

Entgegen erster Vorhaben, bezugnehmend auf benutzerfreundlichkeit, erzwingen wir zukünftig 2-Faktor-Authentifizierung für alle Benutzer.

Entgegen berechtigter Forderungen verzichten wir auf die Schadenspauschale und den Notfallzuschlag und setzen uns dafür für eine Stärkung der Architektur und für eine Härtung aller Systeme ein.

Um zukünftig solche Probleme zu vermeiden hat unseren Krisenstab beschlossen, eine Änderung der Zugriffstruktur zu instruieren. Nach kurzer Planung wurde diese durchaus aufwendige Aufgabe der Umstrukturierung durch unsere IT-Team begonnen und umgesetzt.



i *Dieses Exposee dient als Rechtfertigung der eingetretenen Probleme und der durchgeführten Maßnahmen durch den Dienstleister technik.schächner.de. Er weist auch auf die, zum jetzigen Kenntnisstand inakzeptable Benutzung der SchächnerCloud hin. Maßnahmen werden folgen.*

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

Vervielfältigung sowie Weitergabe und jegliche Kopien elektronischer und analoger Art sind untersagt.

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