Fonte: swz.it
Data: 11/10/2024
Categoria: Raiffeisen-Geldorganisation Print & Web | Link

Rothoblaas: Die Lehren eines Hackerangriffs

swz.it/rothoblaas-die-lehren-eines-hackerangriffs/

11. Oktober 2024

Kurtatsch/Bozen – Es war ein Mittwochmorgen im September. Für Stefan Trebo und die anderen Mitarbeitenden von Rothoblaas hatte der Arbeitstag gerade erst begonnen, als klar wurde: Etwas im Unternehmensnetzwerk stimmt nicht. „Die Kontrolllampen unserer Software für die Überwachung unserer Systeme leuchteten an diesem Morgen vermehrt rot, anstatt wie üblich grün. Als dann immer mehr Probleme auftauchten, wussten wir: Etwas ist faul“, erinnert sich Stefan Trebo, Global Head of ICT (der globale IT-Leiter) bei Rothoblaas. Was war passiert?

Eine Lücke in der Firewall

Während zahlreiche Hackerangriffe in Unternehmen über Phishing-Mails erfolgen, sprich Mails, die Mitarbeitende dazu verleiten, schadhafte Software herunterzuladen oder sensible Daten weiterzugeben, war das bei Rothoblaas nicht der Fall. Dort ging der Angriff von einem Gerät aus, das eigentlich genau vor solchen Angriffen schützen sollte, wie Rai Südtirol kürzlich berichtete.

Das Unternehmen, das in der Entwicklung von Bautechnologie tätig ist, nutzt mehrere Instrumente, um sich vor Cyberangriffen zu schützen. „Eines davon ist ein Gerät, eine Firewall. Dort hat sich ein paar Tage vor dem Angriff eine Sicherheitslücke ergeben – und die

ist prompt ausgenutzt worden“, erklärt Stefan Trebo. Wegen dieser Lücke sei die Hackergruppe über Nacht imstande gewesen, ins Netzwerk des Unternehmens einzudringen und sich auszubreiten.

> „Leider ist es zur Normalität geworden, dass Unternehmen überfallen werden.“ Martin Galler

Den Angriff bemerkt habe das Unternehmen anhand der eingangs erwähnten Monitoringsoftware und aufgrund zunehmender Fehlermeldungen. Viele Programme funktionierten nicht, Inhalte waren verschlüsselt. „Die PCs selbst liefen noch, aber viele unserer Softwares zeigten Fehlermeldungen an. Also haben wir viele der Mitarbeiter nach Hause geschickt“, blickt Trebo zurück.

Nach einiger Zeit habe das IT-Team der Firma auf einem der betroffenen Server eine Textdatei gefunden: eine Nachricht der Hackergruppe. Darin standen die Anweisungen dazu, wie die Daten wieder zugänglich gemacht werden können. „Wir hätten uns über das Dark Web mit der Hackergruppe in Verbindung setzen sollen. Dort wäre uns der Betrag genannt worden, den die Gruppe fordert“, sagt Trebo. Aus internationalen Erhebungen wisse man, dass es sich in der Regel um drei bis vier Prozent des Jahresumsatzes handelt. „Diesen Betrag wollen die Angreifer dann in Bitcoin überwiesen bekommen.“ Das Unternehmen hat sich aber gegen die Überweisung des Lösegelds entschieden. „Wir lassen uns nicht erpressen“, sagt Trebo. Rothoblaas hatte außerdem einen konkreten Plan, wie es sich im Falle eines Angriffs verhalten würde.

Ein Notfall-Meeting mit dem Emergency-Board

„Wir haben in der Vergangenheit bereits einen ‚disaster recovery plan‘ ausgearbeitet, also einen Plan mit vorprogrammierten Abläufen für den Fall eines Angriffs“, erklärt Stefan Trebo. Solche Attacken seien im Unternehmen schon öfter simuliert worden, um das richtige Verhalten im Notfall zu üben.

Gleich nach Bekanntwerden des Angriffs sei das Emergency-Board des Unternehmens einberufen worden. Dort seien alle Abteilungsleiter:innen über das weitere Vorgehen informiert worden.

Derweil habe das IT-Team nach der Lücke im System gesucht, um diese so schnell wie möglich zu schließen. „Dabei werden zuerst alle Systeme vom Netz getrennt. Wenn die Lücke dann geschlossen ist, beginnt man mit der Wiederherstellung des Systems“, so Trebo. Drei Tage dauerte diese Prozedur bei Rothoblaas. Drei Tage stand das Unternehmen still. Und wären die Daten des Unternehmens nicht gesichert gewesen, wäre der Fall möglicherweise anders ausgegangen. Dann hätte das Lösegeld vielleicht bezahlt werden müssen, um die Daten zurückzubekommen.

„Wenn man saubere Back-ups der Daten hat, kann man diese wieder zurückholen. Leider wissen die Hacker, dass viele Firmen in diesem Bereich recht lasch sind und nicht in Back-up-Systeme investieren“, so Trebo. Dann passiere es, dass die Firmen plötzlich ohne Daten dastehen.

Sechs von zehn Unternehmen betroffen

Rothoblaas ist beileibe nicht das einzige Unternehmen, das Opfer eines Hackerangriffs geworden ist. Laut einer Anfang September veröffentlichten Studie des Verbandes der deutschen Informations- und Telekommunikationsbranche (bitkom) erlebten in den zwölf Monaten davor sechs von zehn deutschen Unternehmen einen Angriff mit Ransomware. Bei Ransomware handelt es sich um Schadsoftware, die – wenn die Angriffe aus Sicht der Kriminellen erfolgreich verlaufen – in Netzwerke und auf Computer eingeschleust wird, die Daten verschlüsselt und sie teilweise sogar an die Hackergruppen sendet. Möchten Unternehmen wieder auf die Daten zugreifen und eine Veröffentlichung verhindern, werden sie zu Zahlungen aufgefordert.

1.000 Unternehmen wurden repräsentativ befragt. Von den 60 Prozent, die angegriffen wurden, beklagte etwa die Hälfte keinen Schaden, bei der anderen Hälfte ist hingegen sehr wohl ein Schaden entstanden, etwa durch Produktionsausfall, Kosten für IT-Dienstleister oder auch durch Zahlungen an die Täter. Jedes achte der betroffenen Unternehmen ist auf die Lösegeldforderungen eingegangen, liest man in der Studie.

Die zwei beliebtesten Wege der Kriminellen

Dass es immer wieder zu Hackerangriffen mit schwerwiegenden Folgen für Betriebe kommt, weiß auch Martin Galler. Er ist der Verantwortliche für „Information Security & Privacy“ beim IT-Unternehmen Konverto. „Leider ist es zur Normalität geworden, dass Unternehmen überfallen werden“, stellt er fest.

Die meisten Fälle von Angriffen würden anhand von Phishing-Mails getätigt. „Klickt der Mitarbeitende auf einen Link, wird in der Folge eine Schadsoftware auf dem Computer installiert. Diese breitet sich dann im Unternehmensnetzwerk aus, es sei denn, das Sicherheitssystem funktioniert“, so Galler.

> Während es bis vor einigen Jahren geheißen habe, man solle anschließend die PCs abschalten, laute der Rat mittlerweile: Die Systeme so stehen lassen, wie sie sind.

Eine zweite Methode, wie sich Hackergruppen Zugriff auf Unternehmensdaten verschaffen, sind Lücken im Sicherheitssystem. Galler: „Oft werden Systeme nicht aktualisiert und es fehlen letzte Sicherheitsupdates.“

Opfer von Hackerangriffen seien oftmals große Unternehmen, zunehmend aber auch mittelständische. „Gerade mittlere Unternehmen kümmern sich oft nur wenig um ihre IT-Sicherheit, während große gut geschützt sind."

Was im Notfall zu tun ist

Merkt ein Unternehmen, dass sich Kriminelle Zutritt verschafft haben, sollten mehrere Dinge befolgt werden. „Die Systeme sollten sofort vom Internet getrennt werden. Das heißt: Alle Verbindungen ins Internet müssen abgeschaltet werden", erklärt Martin Galler. Während es bis vor einigen Jahren geheißen habe, man solle anschließend die PCs abschalten, laute der Rat mittlerweile: „Die Systeme so stehen lassen, wie sie sind. So kann untersucht werden, was betroffen ist und was nicht, und die Systeme können voneinander getrennt werden."

Viele Unternehmen würden auch eine Informationssperre nach außen verhängen. So gelangen keine Fehlinformationen an die Öffentlichkeit und die Kommunikation mit der Kundschaft und den Mitarbeitenden kann besser gesteuert werden.

Sobald der Schaden begrenzt und das Problem gefunden ist, gehe es darum, die verlorenen Daten wiederherzustellen. Das kann Tage oder Wochen dauern, sagt Galler. „Hat ein Unternehmen keine Datensicherung oder wurde auch die gestohlen – das wird oft als Erstes versucht –, ist es beinahe gezwungen, das Lösegeld zu zahlen."

Das alles klingt recht einschüchternd, gerade für Unternehmen, die sich bislang wenig mit ihrer Cybersicherheit beschäftigt haben. Martin Galler beschwichtigt: „Es sind nicht viele Maßnahmen, die Betriebe umsetzen müssen. Sie müssen sich nur einmal mit der IT-Sicherheit auseinandersetzen und dann dranbleiben."

Vorbeugen ist besser als Heilen

Wie also können Unternehmen Hackerangriffen vorbeugen? „In der Regel braucht es keine ausgefeilten Sicherheitsmaßnahmen oder große IT-Abteilungen, sondern einige Maßnahmen zur grundlegenden Sicherheit", erläutert Galler. Unternehmen, die diese nicht haben, würden eher zu Opfern werden. „Und wenn Angreifer ein Unternehmen wirklich gezielt kapern wollen, dann finden sie einen Weg."

> „Man sollte nicht nur schauen, was die Software kostet, sondern auch, was der Schutz der Software selbst und der Infrastruktur, auf der sie läuft, kosten." Stefan Trebo

Die „Basissicherheitsmaßnahmen" fußen laut Martin Galler auf drei Säulen:

1. **Technischer Aspekt:** Dazu gehören etwa ein verlässliches Antivirussystem, eine funktionierende Firewall, Sicherheitsmaßnahmen für die Accounts, sichere Passwörter und das Ausmisten alter Softwares. „Wir sehen oft, dass alte Systeme einfach weiterlaufen. Davon raten wir ab", so Galler.

2. **Faktor Mensch:** „In 85 Prozent der Angriffe spielt die menschliche Komponente eine Rolle“, sagt der IT-Experte. Deshalb sei in Unternehmen Sensibilisierung wichtig.

3. **Organisatorische Maßnahmen:** Abläufe in Unternehmen müssen auch aus Sicht der IT-Sicherheit gut organisiert werden. „Ein neuer Mitarbeiter muss nicht gleich alle Zugriffsrechte bekommen, genauso sollte ein Account sofort gesperrt werden, wenn ein Mitarbeiter ein Unternehmen verlässt“, erläutert Martin Galler. Auch die Zugriffsberechtigungen müssten in vielen Fällen überprüft werden: Nicht jede:r müsse Zugriff auf alle Dateien haben.

Neben den Basissicherheitsmaßnahmen sei es wichtig, dass Unternehmen regelmäßige Sicherheitsupdates von Softwares durchführen und Daten-Back-ups an einem sicheren Ort, bestenfalls offline, erstellen.

„Investitionen lohnen sich“

Bei Rothoblaas sei bereits viel in Sicherheitssysteme investiert worden, sagt Stefan Trebo, der globale IT-Leiter des Unternehmens. Das IT-Team bestehe aus 15 Personen, dazu komme das Know-how einer externen Firma, die es im Hinblick auf Cybersicherheit unterstütze. „Aber wir wissen nun: Man kann immer noch Verbesserungen vornehmen.“

Das Kurtatscher Unternehmen sondiere nun, ein neues Sicherheitssystem zu implementieren, bei dem eine künstliche Intelligenz die Netzwerkaktivitäten zusätzlich überwacht, zum Beispiel in der Nacht oder am Wochenende. Überdies werde überlegt, die Leistungen eines Security Operation Centers (SOC) in Anspruch zu nehmen. Dabei handelt es sich um externe Fachleute, die die Cybersicherheit von Organisationen bewachen.

Trebo rät anderen Betrieben, ein Budget für Cybersicherheit vorzusehen. „Man sollte nicht nur schauen, was die Software kostet, sondern auch, was der Schutz der Software selbst und der Infrastruktur, auf der sie läuft, kosten, und dementsprechend investieren.“ Bei Rothoblaas habe sich außerdem der „disaster recovery plan“ als vorteilhaft erwiesen. Trebo: „Es ist wichtig, den Notfall zu simulieren: Was wird konkret getan, wenn es dazu kommt? Wer wird informiert? Gibt es einen Kommunikationsplan?“ Auch in Schulungen der Mitarbeitenden solle investiert werden. „Mein Rat ist, eine Schulungssoftware zu benutzen. Damit kann man simulierte Phishing-Mails verschicken und sehen, wer sich täuschen lassen würde und ob noch Schulungsbedarf notwendig ist.“ Einen hundertprozentigen Schutz vor Cyberangriffen gebe es nicht, sagt Trebo, „aber jede Bemühung in diese Richtung lohnt sich“.

Schlagwörter: 39-24freeTop2

Ausgabe 39-24, Seite 5