Expert Notes

Informieren. Aufklären. Sensibilisieren.

4. Februar 2021 Ausgabe **14.**

Expert Notes. Der regelmässig erscheinende Fachbericht der Neo One zu aktuellen Themen.

Eine Publikation der Neo One.

IT

Das beste Lehrbuch ist bekanntlich die Praxis. Ein Praxisbeispiel, was einem Schweizer KMU Unternehmen bereits in dem noch jungen, laufenden Jahr passiert ist, sollte aufrütteln, wach machen und sensibilisieren. Die Hintergründe sind entscheidend, um die richtigen Lehren auch für Ihr Unternehmen zu ziehen.

Der winterliche Sonntag mit bitterem Nachgeschmack.

Dann, wenn man es am wenigsten erwartet… Das Wetter lädt zum Geniessen ein und die Flocken fallen vom Himmel. Gemütlich könnte der Tag draussen im Schnee oder auf dem heimischen Sofa verbracht werden. Das Telefon klingelt – es ist der Leiter des IT Sicherheitsteams!

Wenn man selbst betroffen ist, bekommt das Wort Notfall eine ganz andere Bedeutung.

«Notfall – wir wurden angegriffen und unsere Systeme werden gerade verschlüsselt!»

Vorbei mit der Sonntagsruhe.

Wow, so schnell kann man aus der Sonntagsruhe gerissen werden und man steht mitten in einer Notfallorganisation. Es geht plötzlich um das Überleben der Firma, um Datenschutz, welcher verletzt wird, um finanzielle Konsequenzen, um Arbeitsplätze und die Reputation.

Wenn Ihr nicht bezahlt, dann…

Was ist passiert. Ein weltweit tätiges Schweizer Produktionsunternehmen wurde von Cyber-Kriminellen ins Visier genommen. Dabei wurde eine Schadsoftware in das Unternehmen geschleust, welche Daten abgezogen und danach die Systeme bzw. die darin gespeicherten Daten verschlüsselt hat. Ein klassischer sogenannter Ransomware-Angriff bei welchem die Daten für das Unternehmen unzugänglich gemacht werden, um das Unternehmen zu erpressen.

«Ohne Lösegeld erhaltet Ihr den Schlüssel für die Entschlüsselung der Daten nicht.»

«Und wenn Ihr nicht bezahlt, veröffentlichen wir die vertraulichen Daten im Internet.»

Eine durchaus heikle Situation. Die Produktionssysteme konnten teilweise unabhängig der IT betrieben werden. Aber wenn kein Computer, kein Server und somit kein Dokument mehr verfügbar ist, dann steht der Betrieb grösstenteils still. Die Frage ist für wie lange und ob überhaupt die notwendigen Daten wiederhergestellt werden können.

Wie kann das denn überhaupt passieren?

Cyber-Kriminelle nutzten einen geklauten Fernzugriffszugang aus, um ins Unternehmensnetzwerk zu gelangen.

NEONE *Rundum. IT bis Digitalmarketing.*

Neo One AG
Grindelstrasse 6
8303 Bassersdorf

+41 43 233 30 30
hello@neo-one.ch
www.neo-one.ch

Einmal im Netzwerk, wurde gezielt nach Schwachstellen gesucht und diese wurden auch gefunden. Dank diesen Schwachstellen erlangte der Angreifer höhere Rechte. Innerhalb mehrerer Tage konnte sich der Angreifer unbemerkt im Netzwerk und auf den Systemen mit einem legitimen Benutzer bewegen und sich einen Überblick über das System und die Daten verschaffen. Entsprechende weitere Schadsoftware konnte ohne Probleme nachgeladen werden und anschliessend starteten die eigentlichen effektiven schädlichen Aktionen:

Daten wurden auf einen Online-Datenspeicher im Internet hochgeladen resp. abgezogen

Daten wurden auf den Unternehmenssystemen verschlüsselt

Kontaktaufnahme mit dem Unternehmen mit der Platzierung des Erpresserschreibens

Wieso blieb der Vorfall unentdeckt?

Die Angreifer waren versiert und hatten die Zeit und das Know-how, um ihre Spuren des Einbruchs, also über die Vorgehensweise, weitestgehend zu bereinigen und blieben so unterhalb des Radars der Systemüberwachungen.

Was hätte präventiv verhindert werden können? Worüber ärgert sich das Unternehmen im Nachhinein?

1. Fernzugriffe waren mit einer Zwei-Faktor-Authentisierung gesichert, aber einige wenige Personen hatten eine Ausnahme, sich nur mit Benutzername und Passwort anmelden zu können!
2. Die Zugangsdaten von mindestens einem Benutzer wurden vermutlich durch eine vorhergehende Phishing-Attacke durch unbekannte Angreifer abgefangen
3. Es wurde eine Software durch das Unternehmen eingesetzt, welche nicht aktuell gepatched war und über bekannte Sicherheitslücken verfügte
4. Ausgehende Verbindungen ins Internet waren nicht, bzw. zu wenig eingeschränkt und somit konnten Daten an den Überwachungstools vorbei und somit unbemerkt ins Internet geladen werden

Wie kann man sich zielsicher schützen?

- Alle Benutzerzugänge sollten mittels einer Zwei-Faktor-Authentisierung geschützt werden
- Das Netzwerk muss kritische Systeme, schwach gesicherte Systeme und solche, welche von extern zugänglich sind, strikt voneinander trennen mit einer entsprechenden Netzwerksegmentierung
- Benutzer müssen mittels Awareness-Trainings im Umgang mit E-Mails, Web und Zugangsdaten geschult werden
- Software, Firmware sowie Betriebssysteme müssen immer auf dem aktuellen Stand sein und bekannte Sicherheitslücken mit den vom Hersteller gelieferten Sicherheitsaktualisierungen umgehend gepatched werden
- Ausgehende Verbindungen vom internen Netzwerk ins Internet müssen stark eingeschränkt und überwacht werden

N-Tipp

Seien Sie vorbereitet, Sie werden es sonst bereuen.

- Umfassendes Backup-Konzept erstellen
- Backup-Daten auf einem Offline-Backup speichern
- Disaster Recovery Plan erstellen
- Trainieren der Notfallabläufe
- Wiederherstellung von Daten aus dem Backup trainieren und prüfen

Michael Schlüter
Senior ICT Security Consultant
& Cyber Security Officer

In einer Kaffeelänge zu mehr Cyber-Sicherheit. Sprechen Sie mit denjenigen, die nicht nur beraten, sondern umsetzen.

cybersecurity@neo-one.ch

Sich im Kleinen mit Informatik zu befassen, heisst immer mehr von unserer digitalen Welt zu verstehen. Machen Sie den ersten kleinen Schritt.

Nice to know

Cyber-Attacke

– Eine Cyber-Attacke oder ein Cyber-Angriff ist der gezielte Angriff auf grössere, für eine spezifische Infrastruktur wichtige Rechnernetze von ausserhalb (insbesondere aus dem Internet) zur Sabotage, Informationsgewinnung und Erpressung.

Verschlüsselung

– Verschlüsselung ist die von einem Schlüssel abhängige Umwandlung von „Klartext" genannten Daten in einen «Geheimtext», so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.

Schadsoftware

– Als Schadprogramm, Schadsoftware oder zunehmend als Malware – englisch badware, evilware, junkware oder malware – bezeichnet man Computerprogramme, die entwickelt wurden, um, aus Sicht des Opfers, unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Der Begriff des Virus ist häufig nicht klar abgegrenzt.

Datensicherung

– Datensicherung bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes wiederherstellen zu können. Somit ist Datensicherung eine elementare Massnahme zur Datensicherheit. Die auf einem Speichermedium redundant gesicherten Daten werden als Sicherungskopie, engl. Backup, bezeichnet.

Schwachstellen

– Eine Schwachstelle bezeichnet in der IT eine Sicherheitslücke welche aufgrund von fehlerhafter Programmierung in Software oder durch fehlerhafte Komponenten in der Hardware entstehen können, welche zu unbefugtem Verändern, Einsehen oder Löschen von Daten sowie Störung der IT Infrastruktur führen kann.

Cyber Kriminelle

Computerkriminalität im Allgemeinen, Straftaten unter Ausnutzung elektronischer Infrastruktur.

Zwei-Faktor-Authentisierung

– Die Mehrfaktor-Authentisierung, häufig auch als Zwei-Faktor-Authentifizierung bezeichnet, bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (z.B. Kennwort und Einmalpasswort).

Phishing Attacke

– Unter dem Begriff Phishing versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es z. B. an persönliche Daten eines Internet-Benutzers zu gelangen oder ihn z. B. zur Ausführung einer schädlichen Aktion zu bewegen.

Disaster Recovery (Plan)

– Der englische Begriff Disaster Recovery bezeichnet Massnahmen, die nach einem Ausfall von Komponenten in der Informationstechnik eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbarer Infrastruktur, Hardware und Organisation.

Michel Hipp
Leitung ICT / Senior ICT System Engineer