FACHLETTER

Sommerliche Hackerattacken: Sicherheit im digitalen Zeitalter

Diesen Sommer hatte eine Welle von Hacking-Angriffen die Schweiz erfasst, welche sowohl in ihrer Art wie auch in den Auswirkungen neue Dimensionen erreichte[i]: Zum einen fielen neben mehreren Grossunternehmen[ii] diesmal auch KMUs der Attacke zum Opfer[iii], zum anderen hatten sie Schäden in Millionenhöhe verursacht und diverse Unternehmen haben über Tage oder Wochen nur im «Notbetrieb» funktioniert[iv]. Es ist davon auszugehen, dass die in den zitierten Artikel genannten Fälle, nur die Spitze des Eisbergs darstellen.

Wie können sich Unternehmen im digitalen Zeitalter gegen solche Angriffe schützen? Project Competence sprach mit zwei Experten der Firmen Netcloud und Baggenstos zum Thema Datensicherheit.

Markus Hegi und Dan Bausch
Project Competence AG

Typischerweise laufen Hacking-Angriffe heute in drei Phasen ab[v]:

› Phase I: Hacking-Angriff/Zugriff verschaffen
Zuerst verschaffen sich die Hacker Zugriff auf ein Konto und einen PC im Unternehmen. Dies geschieht oft über ein «Randsomware»-Email: Diese haben in Bezug auf die Fälschungsqualität auch im Schweizer Umfeld eine neue Dimension erreicht und sind immer besser und echter gemacht. Es kann also grundsätzlich jedes Schweizer Unternehmen treffen[1]. Diese «Unternehmenszugriffe» werden dann auch im «Darknet» weiterverkauft.

[1] Wir hatten einen Fall bei einem Kunden, in welchem eine Partnerfirma gehackt wurde: Die Hacker haben dann versucht, von der gehackten Firma aus, weitere Firmen zu infizieren. Sie taten dies, indem sie Mails von der Domäne der gehackten Firma versandten, als Antwort auf Mails, die unser Kunde gesendet hatte.

› Phase II: Analyse und Infizierung
Als nächstes analysieren die Hacker die Infrastruktur des Unternehmens und versuchen, möglichst viele weitere Maschinen zu infizieren. Via den einen infizierten PC laden die Hacker diverse Schadenssoftware nach. Häufig bewegen sich die Hacker über Monate in den Firmennetzen, ohne dass von diesen Aktivitäten bei den Unternehmen etwas wahrgenommen wird.

› Phase III: Verschlüsselung/Wiping
Ist die Kontrolle über alle wichtigsten Systeme einmal erfolgt, dann folgt typischerweise in der Nacht oder an einem Wochenende die Verschlüsselung oder das Wiping der Daten, meist zuerst die Backups, sowohl lokal wie auch in der Cloud.

Dies ist die Kehrseite der Medaille einer vollständigen Vernetzung. Soviel Vorteile und Chancen zu neuen Geschäftsmodellen eine effiziente Digitalisierung einerseits bringt, verlangt sie anderseits auch eine neue Sicht auf die Datensicherheit. Etablierte Modelle genügen den Anforderungen nicht mehr.

Diese Herausforderung hat auch im Kreis unserer Kunden zu zahlreichen Fragen in Bezug auf den Umgang mit Datensicherheit geführt.

Um diese Fragen umfassend zu beantworten, unterhielten wir uns deshalb mit Marc Zimmermann (Firma Netcloud) und Eckhard Neuhaus (Firma Baggenstos), welche in den vergangenen Wochen als Experten wiederholt mit der Thematik konfrontiert wurden, über die drei Themengebiete: Wie schützt man sich im digitalen Zeitalter? Wie sicher ist die Microsoft Cloud und Office 365? Wie kann man im «Worst Case» die Daten möglichst schnell wiederherstellen?

Bei einem Totalverlust aller relevanten Informationen eines Unternehmens geht es nicht mehr nur um finanziellen Schaden, sondern oft um die Existenz des Unternehmens. Wie schützt man sich im digitalen Zeitalter vor diesem «Worst Case»?

(Marc Zimmermann): «Die Antwort auf diese Frage ist im «Digitalen Zeitalter» dieselbe wie zuvor. Der Kunde hat die Verantwortung für seine Daten und muss ein solides Backup-Konzept haben. Für den Kunden neu ist die Tatsache, dass diese Konzepte sich nicht mehr nur auf lokale Daten beschränken. Es gilt auch diejenigen Daten, welche in einer Cloud liegen, umfassend zu sichern.
Neben dem Backup der Daten sollten sich aber auch proaktive Fragen gestellt werden, wie der Kunde den Totalverlust seiner Daten möglichst verhindern kann. Hier unterstützen wir unsere Kunden bereits heute mit einem Cyber-Defence-Center-Service, um gegen die Gefahren einer Cyberattacke gewappnet zu sein.»

(Eckhard Neuhaus): «Der Stand der heutigen Digitalisierung hat den Anspruch, dass Mitarbeiter zu jeder Zeit mit den unterschiedlichsten Geräten von überall her arbeiten können. Um diesem Anspruch zu genügen, reichen etablierte Schutzmechanismen, wie eine gute Firewall oder Proxy-Dienste, nicht mehr aus.
Ein zeitgemässes Schutz-Konzept muss die beiden Schwerpunkte «Identität» und «Daten» abdecken. Um sicherzustellen, dass Login-Daten von Mitarbeitern nicht missbraucht werden, geben die Cloud-Services uns viele wirksame Tools in die Hand. Zum Bespiel sollte eine Multifaktor-Authenifizierung (MFA)[2] genauso zum Einsatz kommen, wie «Advanced Threat Analytics» (ATA)[vi] bei der ein selbstlernendes System bewertet, ob das Verhalten eines Logins als regulär eingestuft werden kann oder nicht. Ergänzend zu den Backups werden Daten heute vor allem durch wirksame Kontrollen geschützt, welche Applikationen überhaupt auf welche Daten zugreifen dürfen und welche nicht.»

Viele Unternehmen sind mittlerweile auf Office 365. Wie sicher sind eigentlich die Daten auf dem «Exchange online», dem «OneDrive» und dem «online SharePoint»?

(Eckhard Neuhaus): «Grundsätzlich sind Daten bei O365 gut aufgehoben. Es gibt wenig Firmen, die so viel in Sicherheit investieren, wie Microsoft. Es gibt nicht nur SLAs auf den Services selbst, sondern auch eine Versionierung der Daten. Ergänzend gibt es gute Tools, mit denen

[2] Multifaktor-Authentisierung, ist eine Verallgemeinerung der Zwei-Faktor-Authentisierung, bei der die Zugangsberechtigung durch mehrere unabhängige Merkmale (Faktoren) überprüft wird. Ein gängiges Beispiel ist ein Login via Passwort und SMS-Code.

die Kunden ihre Daten aus O365 zusätzlich sichern können.»

(Marc Zimmermann): «Die Frage nach «wie sicher» die Daten in der Microsoft-Cloud sind, ist letztlich eine Frage des Vertrauens zur Firma Microsoft. Microsoft bietet für die O365-Services eine sehr hohe Verfügbarkeit der Services und der Daten an. Die Verantwortung für die Daten bleibt jedoch beim Kunden selbst. Um diesem Umstand gerecht zu werden empfehlen wir unseren Kunden seine Office-365-Daten ergänzend mittels einer Backup-Lösung auch ausserhalb der Microsoft-Cloud zu sichern.»

Auch wenn man sichergestellt hat, dass ein Backup der wichtigen Daten auf jeden Fall vorhanden ist, dauert es oft Tage und Wochen, diese Daten wiederherzustellen und alle Systeme neu aufzubauen. Welche Massnahmen sind heute «Best Practice», um diesen Fall zu verhindern?

(Eckhard Neuhaus): «Am Anfang steht eine Bewertung, welche Systeme für eine Unternehmung vital sind, und wie lange ein Kunde auf welche Services oder Daten verzichten kann. Basierend auf diesen Aussagen kann mit dem Kunden seine optimale «Disaster Recovery»-Strategie festgelegt werden. Auch hier können Cloud-Services mit etablierten Systemen die Hand reichen. So kann z.B. «Azure Site Recovery» Server direkt nach Azure spiegeln. Azure betriebene Systeme können automatisiert wieder neu aufgesetzt werden, um die benötigte Zeit deutlich zu verkürzen. Entscheidend für eine erfolgreiche «Disaster Recovery»-Strategie ist es, dass die geplanten Massnahmen in regelmässigen Tests validiert werden.»

(Marc Zimmermann) «Die Frage ist letztlich welche Werte für die RTOs (Recovery Time Objectives) und RPOs (Recovery Point Objectives) definiert werden, mit anderen Worten, wie viele Daten darf ich im Fall eines Desasters maximal verlieren und wie lange darf eine Wiederherstellung maximal brauchen. Diese Werte müssen nicht zwingend für alle Systeme gleich sein. Businesskritische Systeme werden anders behandelt als unkritische Systeme. Diese Werte bilden die Basis für ein solides Recovery-Konzepts.
Um den Fall zu verhindern, dass die Wiederherstellung Tage oder Wochen braucht, macht es Sinn seine Backup-Daten in einer Cloud zu halten, in welcher auch eine Wiederherstellung dieser Daten möglich ist. Das heisst der Cloud-Provider hält die Ressourcen für den Fall eines Desasters bereit und erlaubt damit die Daten schnell «lokal» wiederherzustellen, ohne diese über Tage oder Wochen wieder zurückkopieren zu müssen.
Wir beraten unsere Kunden in der Erstellung von «Disaster Recovery»-Konzepten, welche weit mehr als nur die Wiederherstellung der Daten berücksichtig. Auch das Thema Benutzerzugriff, Automatisierung, Wiederherstellungsabhängigkeiten usw. muss betrachtet werden.»

KONTAKTE

› Markus Hegi und Dan Bausch
Project Competence AG www.project-competence.com
M: m.hegi@project-competence.com, d.bausch@project-competence.com T: +41 44 943 70 40

› Eckhard Neuhaus
Baggenstos & Co. AG www.baggenstos.ch
M: eneuhaus@baggenstos.ch T: +41 44 832 66 66

› Marc Zimmermann
Netcloud AG www.netcloud.ch
M: zimmermann@netcloud.ch T +41 58 344 12 12

[i] https://www.nzz.ch/wirtschaft/schweizer-firmen-vermehrt-mit-verschluesselungs-trojanern-attackiert-ld.1499064
[ii] https://www.srf.ch/news/wirtschaft/geht-es-um-loesegeld-hacker-legen-schweizer-grossunternehmen-lahm
[iii] https://www.netzwoche.ch/news/2019-08-05/crealogix-faellt-cyberkriminellen-zum-opfer
[iv] https://www.nzz.ch/wirtschaft/cyber-angriff-auf-schweizer-firma-offix-ein-kampf-ums-ueberleben-ld.1492862
[v] https://www.inside-it.ch/articles/54898
[vi] https://www.microsoft.com/de-ch/microsoft-365/enterprise-mobility-security/advanced-threat-analytics?rtc=1