GLOBAL SYSTEM®
YOUR IT-SOLUTION PROVIDER

Global System informiert – 2. Quartal 2017

Sehr geehrte Kundin, sehr geehrter Kunde

In den letzten Wochen haben einige Internetangriffe Schlagzeilen gemacht. Immer mehr Verschlüsselungstrojaner sind im Umlauf und die Tricks mit denen versucht wird Opfer zu täuschen, sind zum Teil nur noch schwer als solche zu erkennen.

Wir sind mit Sicherheitsexperten einig, die weltweite Situation wird sich bezüglich Internetattacken nicht mehr beruhigen. Die Internetkriminalität wird zusehends professioneller, die Attacken immer ausgeklügelter und vor allem immer stärker.

Auch unser eigenes Datacenter wurde Ziel eines Cyber-Angriffs. Am Dienstag, 30. Mai 2017 gab es einen besonders starken Angriff auf unsere Datacenter-Infrastruktur. Dank unserer Sicherheitsvorrichtungen konnte der eigentliche Angriff abgewehrt werden. Trotz schneller Gegenmassnahmen gestaltete sich die Stabilisierung des Systems schwierig und zeitaufwendig.

Trotz Georedundanz, Cluster-Systemen (Redundante Server) und sehr starker Hardware, kam es bei einigen Kunden stellenweise zu Ausfällen der Telefonie. Die Aufrüstung unserer Abwehrfähigkeiten ist bereits realisiert, damit in Zukunft ein solcher Angriff keine Folgen mehr haben wird. Dieser Fall zeigt, dass selbst wir nicht vor Internetangriffen verschont bleiben.

DDoS-Angriffe

Ein gutes Beispiel dafür sind DDoS-Attacken (DDoS = Distributed Denial of Service). Dabei erhält das Opfer (meistens ein Server) gleichzeitig tausende von Anfragen von anderen Computern, und zwar über Stunden oder Tage hinweg. Ist die Anfrageflut gross genug, kommt der Server nicht mehr nach mit Abarbeiten. Für einen Anwender der nun auf den Server zugreifen will, ist dieser nicht mehr erreichbar.

Das mag nicht so schlimm sein, wenn auf dem Server lediglich Ihre Firmenwebseite betrieben wird. Aber für ein Unternehmen, das von ihrem Online-Shop lebt oder ein Lieferservice der seine Boten über einen Webserver mit aktuellen Daten und Zielen versorgt, wäre ein Ausfall eine Katastrophe vielleicht sogar existenzbedrohend.

Solche DDoS-Attacken werden mit Hilfe von sogenannten Bot-Netzen ausgeführt. Die Grösse dieser Bot-Netze und damit Ihre Fähigkeit selbst die stärksten Server irgendwann in die Knie zu zwingen, nimmt von Jahr zu Jahr zu. Es gibt inzwischen Bot-Netze mit mehreren zehntausend Geräten.

Die Anzahl der täglichen Angriffe weltweit ist überwältigend, mehrere hunderttausend pro Tag. Auf der Webseite www.fireeye.com können Sie sich ein Bild der momentanen Lage machen, dort werden Angriffe visuell in Echtzeit dargestellt.

Die einzelnen Computer die diese Anfrageflut ausführen (sogenannte Bots), wissen nicht, dass Sie infiziert und damit Teil eines Bot-Netzes sind. Ohne ausgereifte Sicherheitsstrategie ist in der heutigen Zeit ein Unglück vorprogrammiert.

Verschlüsselungstrojaner

Der Verschlüsselungstrojaner WannaCry der am Wochenende des 21. Mais die ganze Informatikwelt in Atem hielt, ist das neuste Beispiel. Er hat eindrücklich demonstriert wie schnell sich Schadsoftware in ungenügend geschützten Systemen ausbreiten kann.

Ein Verschlüsselungstrojaner hatte dabei weltweit ganze Systeme lahmgelegt. Sobald ein solches Programm gestartet wird, beginnt es Dateien auf dem System zu verschlüsseln. Die Dateien können danach nicht mehr gelesen oder bearbeitet werden. Nur mit einem passenden Schlüssel können sie wieder entschlüsselt werden und dieser Schlüssel ist in den Händen der Angreifer.

Die Erpresser fordern ein Lösegeld, damit die Daten wieder entschlüsselt werden., meistens in Form von Bitcoins. Wir

raten davon ab Lösegeld zu zahlen, auch wenn einige Kriminelle die Daten nach erfolgreicher Zahlung tatsächlich teilweise wieder freigegeben haben. Eine Garantie gibt es nie. Wer zahlt wird höchstwahrscheinlich auf einer Liste von zahlungswilligen Opfern landen, was die Wahrscheinlichkeit erhöht erneut Ziel von Angriffen zu werden.

Was soll man sonst tun? Wenn Sie regelmässig Backups Ihrer Daten durchführen, können Sie eine vorherige Version Ihres Systems wiederherstellen lassen. Bei kurzen Backupintervallen, werden Sie kaum Daten verlieren.

Ausserdem beginnen Sicherheitsfirmen nach Entdeckung eines neuen Verschlüsselungstrojaners diesen genau zu analysieren. Manchmal ist die Machart dieser Trojaner nicht sonderlich ausgereift und es werden Wege gefunden, die Verschlüsselung rückgängig zu machen.

In jedem Fall sollten Sie es den Behörden melden, Verschlüsselungstrojaner sind eine Form der Erpressung.

Wer steckt hinter solchen Angriffen?

Das Ausführen von einfachen Internetangriffen ist heutzutage nicht mehr schwierig. An den richtigen Orten im Internet kann man fertige Virenbaukäste kaufen. Das Spektrum an möglichen Tätern ist daher sehr breit, es lassen sich aber ganz grob folgende Arten von Angreifer ausmachen:

- Junge Leute die die Kunst des Programmierens noch nicht gemeistert haben, aber genug Halbwissen besitzen um primitive Viren zu schreiben oder die Viren von anderen zu kopieren. Meistens wollen Sie Anerkennung unter Gleichgesinnten erlangen oder Ihr eigenes Ego aufpäppeln.
- Erfahrene Programmierer mit ausgeprägtem Wissen über Netzwerktechnik und Betriebssysteme. Ihnen geht es hauptsächlich ums Geld. Es können Einzeltäter sein oder Hackergruppen. In einzelnen Fällen kann es auch der Geheimdienst eines Landes sein.
- In vielen Fällen werden auch kriminelle Organisationen oder sonstige Terrornetzwerke dahinter vermutet.

Auf Grund der Professionalisierung der Internetkriminalität, können Hacker heute auch Geld verdienen ohne selber direkt Computer und Netzwerke anzugreifen, in dem sie ihre Hackerwerkzeuge auf dem Schwarzmarkt verkaufen oder ihr Bot-Netz vermieten.

Wie kann man sich schützen?

Wir empfehlen:

- Aktivieren Sie die automatischen Windows Updates.
- Installieren Sie einen Virenscanner.
- Verwenden Sie eine korrekt konfigurierte Hardware Firewall.
- Erstellen Sie regelmässig Backups all Ihrer wichtigen Daten.
- Lagern Sie Backups an einem sicheren Ort und nicht angeschlossen an einen Computer. Damit stellen sie sicher, dass Ihre Backups nicht automatisch befallen werden, sollte Ihr Computer infiziert werden.
- Bevor Sie Backups zurückspielen stellen Sie sicher das der befallene Computer 100% gesäubert ist oder sie riskieren, dass Ihr Backup nach dem Anschliessen auch befallen wird.
- Seien Sie sehr vorsichtig im Umgang mit E-Mails von unbekannten Absendern oder wenn Ihnen der Inhalt eines E-Mails suspekt ist.
- Beachten Sie unsere Richtlinien zum Umgang mit E-Mails.
- Sollten Sie beim Öffnen eines Anhangs Sicherheitsmeldungen erhalten (z.B. bei Word- oder PDF-Anhängen), die Sie zum Aktivieren einer Funktion auffordern, stellen Sie sicher, dass es eine legitime Anfrage ist. Wenn Sie das nicht beurteilen können, wenden Sie sich an einen Experten, bevor Sie etwas anklicken.

Wir möchten festhalten, dass es keine 100% Sicherheit gibt und auch nie geben wird. Die Sicherheitsindustrie ist im Moment in einem Wandel, nicht nur Angriffe zu verhindern, sondern auch sicherzustellen, dass ein System schnell wieder einsatzfähig ist, sollte es doch zu einem Zwischenfall kommen.

Mit den obigen Massnahmen, kann man das Restrisiko auf ein Minimum reduzieren. Und mit entsprechenden Wiederherstellungsmassahmen schon nach kurzer Zeit wieder einsatzbereit sein.

Ein vollumfängliches IT-Sicherheitskonzept ist heutzutage integraler Bestandteil einer erfolgreichen Unternehmensstrategie. Es darf auf keinen Fall vernachlässigt werden.

Ich entschuldige mich in aller Form, dass es bei einigen Kunden zeitweise Ausfälle unserer Datacenter-Dienstleistungen gegeben hat. Sie können sicher sein, dass wir alles in unserer Macht Stehende unternehmen, um solche Angriffe in Zukunft noch besser abwehren zu können.

Freundliche Grüsse
Jean-Claude Hasler, CEO

Global System AG – Lerchenweg 1, 4303 Kaiseraugst
Tel +41 61 515 55 55 info@globalsystem.ch

Im Netz:

Falls Sie in Zukunft keine Informationen mehr wünschen, können Sie den Newsletter hier abbestellen.