Strategie-Impulse 11-2017

Dr. Heiko Heinrich Stutzke
stutzke@das-strategiebuero.de

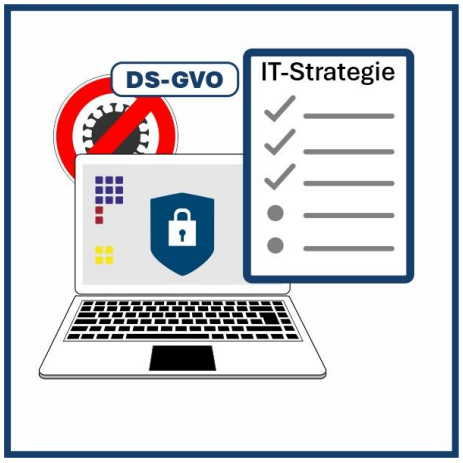
Mai 2017

Download:
Diesen Beitrag können Sie auf unserer Homepage im Bereich „Strategie-Impulse“ als PDF-Datei herunterladen.

IT-Strategie – für Ihre Sicherheit wichtiger denn je!

Die Sonne scheint warm vom Frühsommer-Himmel, und der Gedanke an den nahen Feierabend beflügelt die Stimmung. Niemand im Unternehmen merkt, dass sich gerade ein Überfall anbahnt.

Das ist auch kein Wunder, denn der Angreifer kommt nicht einfach durch die Eingangstür: Er versteckt sich geschickt in den Daten, die permanent als Mails und Dokumente im firmeninternen Netz und mit den externen Partnern ausgetauscht werden. Darin lässt er sich treiben und wartet auf die Gelegenheit, aktiv zu werden. Dann allerdings geht es ganz schnell: Die Festplatten der PCs werden mit einem geheimen Code verschlüsselt, der Datenzugriff ist nicht mehr möglich, und der Betrieb steht still. Auch die externe Kommunikation funktioniert nicht mehr. Eine auffällige Fehlermeldung auf den Monitoren bietet an, gegen Bezahlung eines Betrags in Bitcoin den Entschlüsselungscode zu erhalten.



Dass dieses Erpressungs-Szenario kein Hirngespinst ist, haben wir vor einigen Wochen gesehen, als zahlreiche Windows-PCs in aller Welt vom „Wannacry“-Trojaner „infiziert“ und lahmgelegt wurden. An vielen Stellen wurde die Steuerung der Infrastruktur massiv gestört. Wo gerade noch die pünktliche Personenbeförderung (Bahnbetriebe), die Patientenversorgung (Krankenhäuser) oder die Bearbeitung von Aufträgen (Unternehmen) im Vordergrund stand, ist jetzt Krisenmanagement angesagt. Im Normalfall entstehen dadurch massive zusätzliche Kosten.

Wie konnte das passieren?

Zur Beruhigung mag beitragen, dass mehrere Fehler zusammengekommen sind, welche die „Wannacry“-Attacke erst möglich gemacht haben:

- **Fehler 1: Sicherheitslücke entdeckt, aber nicht gemeldet.** Eine Mutmaßung der Medien be-

sagt, dass die NSA schon vor längerer Zeit eine Sicherheitslücke in früheren Windows-Versionen entdeckt hatte. Um sie für eigene Zwecke ausnutzen zu können, wurde sie nicht an Microsoft gemeldet. Hacker sollen schließlich Hinweise auf die Lücke in NSA-Unterlagen gefunden und den „Wannacry"-Trojaner gebaut haben, um den Angriff zu starten.

- **Fehler 2: Veraltete Windows-Versionen nicht ersetzt:** Die aktuelle Windows-Version 10 war gegen den Eindringling immun. Infiziert wurden nur Rechner, die noch mit veralteten Windows-Versionen (7 und 8 sowie Vista und XP) ausgestattet waren. Windows XP war von Microsoft nach dem Erscheinen am 25. Oktober 2001 mehr als 12 Jahre lang mit Updates unterstützt worden. Das Supportende zum 8. April 2014 wurde lange Zeit vorher in den Medien angekündigt. Niemand kann also sagen, er habe es nicht gewusst. Der Umstieg auf eine aktuelle Windows-Version wurde jedoch von vielen Nutzern nicht durchgeführt. Übrigens: Für Windows Vista ist der Support am 11. April 2017 ausgelaufen; für Windows 7 (mit Service Pack 1) endet er am 14. Januar 2020.
- **Fehler 3: Windows-Updates von Anwendern ignoriert:** Microsoft hatte bereits im März 2017 – also deutlich vor dem Angriff – ein Update für Windows 7 herausgegeben, das die Lücke geschlossen hat. Viele Nutzer hatten dieses Update aber schlicht nicht installiert.

Man könnte also jetzt feststellen, dass sich Murphy's Law wieder einmal bewahrheitet hat, *„Shit happens"* sagen und zur Tagesordnung übergehen.

Auf unsere Verantwortung!

Ganz so einfach ist es aber nicht. Die Verantwortung für solche Vorfälle liegt nämlich nicht nur bei den Tätern – sondern auch bei uns allen.

Ein infizierter Rechner ist für den betroffenen Anwender oder das Unternehmen wahrhaftig schlimm genug. Neben dem lokal angerichteten Schaden wirkt ein solches Gerät aber gleichzeitig fast immer als „Virenschleuder" und versucht aktiv, weitere Rechner zu erreichen und zu verseuchen. Das passiert dann direkt in Ihrem Verantwortungsbereich, wenn Ihre Geräte von einem Virus, einem Trojaner oder einem anderen Schädling betroffen sind. Die meisten Internetanbieter haben Mechanismen entwickelt, um solche Virenschleudern über kurz oder lang zu entdecken. Der entsprechende Kunde erhält dann in der Regel eine Aufforderung, das Problem sehr kurzfristig (!) zu beheben; anderenfalls wird der Internetzugang gesperrt. Das sollte man besser nicht riskieren.

Dass viele Anwender noch immer mit Windows 7 oder sogar Windows XP arbeiten, ist zum Teil sicher der Tatsache geschuldet, dass beide System sehr stabil und angenehm in der Bedienung waren. Insoweit ist es durchaus verständlich, dass der Umstieg schwerfällt. Hinzu kommt, dass die Systeme manche „Sonderlocken" enthielten, die nicht immer so ganz gültigen Normen entsprachen und dafür gesorgt haben, die eine oder andere Spezialsoftware zum Laufen zu bringen. Beim Umstieg auf eine neue Windows-Version können dann Schwierigkeiten entstehen. Aber: Zu einem großen Teil sind es schlicht und ergreifend Bequemlichkeit oder Aufwandaspekte („läuft ja noch"), wenn auf den Schritt zur neuesten Windows-Version (und häufig selbst die Installation von Updates) verzichtet wird.

Wer nutzt ein 16 Jahre altes Mobiltelefon?

Kaum einer von uns hat ein Mobiltelefon, das älter ist als zwei Jahre. Wir achten darauf, immer die neuesten Funktionen zu bekommen, damit alle Apps problemlos laufen und unsere 24-Stunden-Erreichbarkeit unter allen Umständen gewährleistet ist. Beim PC scheint das nicht so wichtig zu sein – darauf kann offenbar ruhig ein 16 Jahre altes Betriebssystem laufen, das auf die Sicherheitsanforderungen der heutigen Zeit überhaupt nicht vorbereitet ist. Es stört auch nicht, dass auf solchen Geräten manchmal kritische oder sensible Unternehmensdaten gehalten und verarbeitet werden.

Schon seltsam, oder?

Übrigens gibt es auch bei den meisten Mobiltelefonen riesige Probleme mit der Sicherheit: Neue Versionen und (Sicherheits-)Updates erscheinen zwar regelmäßig, und zwar sowohl für iPhone und Windows Mobile als auch für Android. Bei Android müssen diese jedoch zunächst aktiv von den Geräte-Herstellern an die jeweiligen Geräte und deren Benutzeroberflächen gepasst werden. Hierdurch geht viel Zeit verloren, und die unüberschaubare Anzahl verschiedener Bedienkonzepte macht die Update-Versorgung praktisch unmöglich. Dementsprechend bekommt der überwiegende Teil der im Umlauf befindlichen Android-Mobiltelefone Updates gar nicht oder nur mit langer zeitlicher Verzögerung. Ihre Benutzerdaten, Kontakte, Bewegungsprofile, Fotos etc. sind also einem enormen Risiko ausgesetzt. Verlust und Missbrauch sind Tür und Tor geöffnet. Auch der geschäftliche Einsatz von Android-Geräten sollte genau überlegt werden.

Was also ist zu tun?

Jeder von uns hat die Verantwortung für die von ihm genutzten oder betreuten Geräte. Diese Verantwortung kann auch nicht an die Hersteller oder an Microsoft delegiert werden. Wir müssen selbst dafür sorgen, dass das Gerät immer alle aktuellen Sicherheits-Updates erhält, und zwar direkt nach deren Erscheinen. Das bedeutet:

- **Bringen Sie Ihre Geräte auf den neuesten Stand des Betriebssystems** – im Falle von Windows also Windows 10 mit den neuesten Updates. Windows 10 spielt die meisten Updates inzwischen automatisch ein und hat dadurch wohl schon manchen Schaden verhindert. Administratoren können zudem über Werkzeuge dafür sorgen, dass betriebliche Prüfungen und Abläufe eingehalten werden. Wenn bei Ihnen Spezialsoftware betroffen ist, sprechen Sie mit dem Anbieter – oder mit Microsoft – über Möglichkeiten der Anpassung an die aktuelle Windows-Version. Übrigens ist Windows 10 sehr stabil, lässt sich komfortabel mit Tastatur, per Touchscreen oder Stift bedienen und ist deutlich moderner als Windows 7 oder gar XP.
- **Sorgen Sie für einen jederzeit aktuellen Virenschutz**, zum Beispiel von Norton, Kaspersky oder einem der anderen großen Anbieter. Wenn Sie bisher kostenlose Software verwenden: Überlegen Sie, ob das Schutzniveau dieser Software wirklich ausreicht.
- **Überprüfen Sie Ihre Datensicherung**. Von einem Trojaner verschlüsselte Daten lassen sich am einfachsten wiederherstellen, indem sie aus einer aktuellen Sicherung zurückgespielt werden. „Aktuell“ bedeutet dabei in der Regel, dass mindestens täglich eine Sicherung

durchgeführt wird.

Diese Maßnahmen reduzieren das Risiko, bei einer neuen Attacke zu den Betroffenen zu gehören, ganz erheblich. Natürlich ist Aufwand damit verbunden – aber der lohnt sich!

Eine gute Strategie zu haben bedeutet, sich aktiv und mit zielgerichteten Maßnahmen auf kommende Herausforderungen einzustellen. Das gilt auch für die IT.

Dann wird die Vorfreude auf den nahenden Feierabend noch schöner.

Redaktionelle Hinweise

Über den Autor

Dr. Heiko Heinrich Stutzke ist Diplom-Ökonom und Geschäftsführender Gesellschafter des Strategiebüros.

Wir moderieren Planungsprozesse - einschließlich Vorbereitung und Dokumentation. Von einer einzelnen Fragestellung bis zur Strategischen Unternehmensplanung. Unsere Kunden sind Unternehmen und Organisationen im privaten, sozialen und öffentlichen Bereich, Firmen am Anfang ihrer Entwicklung und Gründer.

Hinweis zur verwendeten Sprache

Sprachliche Grundlage für unsere Beiträge ist das amtliche Regelwerk des Rates für deutsche Rechtschreibung. Wir sprechen alle Menschen an.

Lobbyregister

Das Strategiebüro ist unter der Kontonummer K4126147 im Lobbyregister des Deutschen Bundestages eingetragen.

Nutzungsrechte

Alle Rechte für unsere Beiträge und die verwendeten Bilder liegen, soweit nicht ausdrücklich anders gekennzeichnet, bei der Das Strategiebüro GbR.

Wir freuen uns, wenn Sie Beiträge und Bilder für Ihre persönliche (ausschließlich private) Information nutzen, sie zitieren oder verlinken. Wenn Sie unsere Beiträge, Bilder oder andere Inhalte jedoch außerhalb der Grenzen des Urheberrechtes ganz oder teilweise für gewerbliche oder hoheitliche Zwecke verwenden, in elektronische Medien einstellen oder weitergeben wollen, bitten wir Sie, hierfür unsere schriftliche Genehmigung einzuholen.