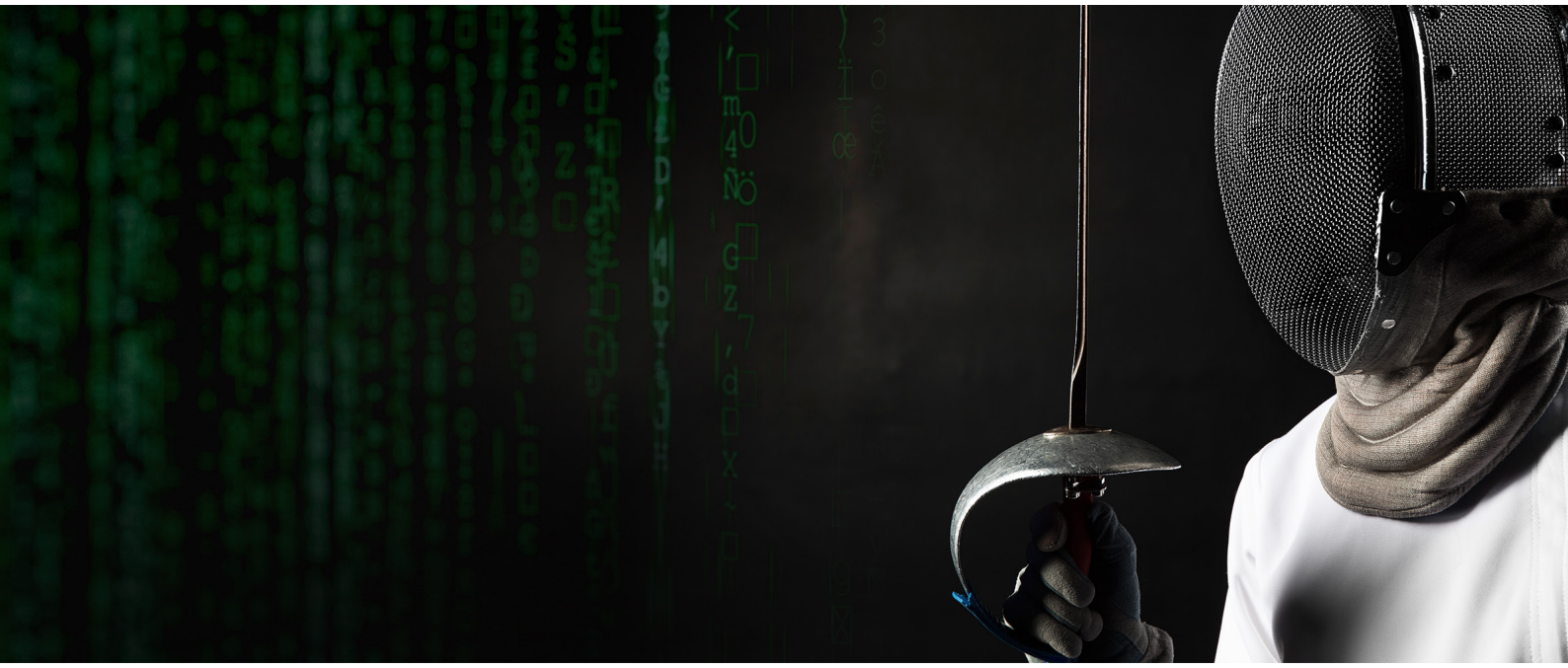
netcos GmbH
Richard-Strauß-Straße 71, 81679 München
Tel.: +49 (89) 45 22 16-0
ww.netcos.de



So ein Szenario konnte man sich vorher gar nicht vorstellen!

Stanislaw Panow über die Relevanz eines vielschichtigen IT-Sicherheitskonzepts

Sicherheitsvorfälle bei seinen Kunden konnte der Geschäftsführer der netcos GmbH in der Vergangenheit stets damit lösen, das Backup zurückzuspielen. Doch ein sonntäglicher Anruf seines langjährigen Business-Partners, dass er einen Sicherheitsvorfall habe und seine IT-Abteilung Unterstützung bräuchte, änderte diese Vorgehensweise schlagartig.

„Als ich hörte, dass die Angreifer auch das Backup gelöscht haben bevor alles andere verschlüsselt wurde, schrillten bei mir alle Alarmglocken. Ich habe mich sofort auf den Weg gemacht, um unseren Partner in dem Krisenfall bestmöglich zu betreuen.“, erinnert sich Panow. Als er nach kürzester Zeit vor Ort eingetroffen war, traf er dort, neben der IT-Mannschaft staatlich gesandte Forensiker an. Alle weiteren Mitarbeiter wurden bereits nach Hause geschickt, da die Systeme des Partners komplett stillstanden.

Nachdem die IT-Experten erfolglos noch einmal geprüft hatten, ob sie das Backup zurückspielen können, mussten sie eine Strategie für das weitere Vorgehen entwicken. „Man konnte sich vorher so ein Szenario gar nicht vorstellen.“, so Panow. „Aus unserer Sicht war das Backup unter anderem auch dadurch sicher, dass man in zwei verschiedene Rechenzentren genutzt hat, die geo-redundant ausgelegt sind. Die Angreifer haben es trotz aller Vorsichtsmaßnahmen – wahrscheinlich durch Brute-Force – geschafft, die Datensicherungen zu verschlüsseln und die zweite, nicht auf Widows-Systemen basierende Sicherung, zu löschen.“

netcos GmbH
Richard-Strauß-Straße 71, 81679 München
Tel.: +49 (89) 45 22 16-0
ww.netcos.de

Nach intensiven Gesprächen entschied sich das knapp tausend Mitarbeiter starke Unternehmen entgegen der Empfehlung der staatlichen Stellen dazu, das Lösegeld zu zahlen. Im Vordergrund stand für die Geschäftsführung ganz klar, die zu 100 Prozent von IT abhängige Organisation zu retten.

Doch wie überweist man möglichst schnell eine erhebliche Summe Geld, wenn man noch kein Bitcoin Wallet hat und auch nicht der Geldwäsche beschuldigt werden möchte?

„Es hat sich eine ganze Industrie gebildet. Mittlerweile existieren Firmen, die solche Dinge treuhänderisch übernehmen und zwischen Erpresser und Unternehmen agieren. Sie überweisen nicht nur das entsprechende Lösegeld, sondern prüfen zusätzlich auch die Entschlüsselungssoftware auf deren Funktionalität und mögliche Backdoors." erklärt Stanislaw Panow.

Balanceakt zwischen Schnelligkeit und Sicherheit

Eineinhalb Tage nach Überweisung lag die Entschlüsselungssoftware vor. Nun musste das weitere Vorgehen sowie dessen Reihenfolge genau abgestimmt werden, denn alle Systeme waren nach wie vor infiziert und die Backdoors des Angreifers noch vorhanden. Zudem bestand ein Interessenskonflikt zwischen dem Unternehmen und den staatlichen Forensikern, da diese vor dem Hochfahren der Systeme zunächst alle Spuren sicherstellen wollten – das Unternehmen jedoch möglichst schnell wieder arbeitsfähig werden wollte.

Diese Uneinigkeit entschied sich schließlich zu Gunsten des Unternehmens, sodass schnellstmöglich ein Krisenmanagement etabliert und ein Dutzend externer IT-Experten engagiert wurden, die beim Wiederaufbau der Systeme unterstützten. „Das Kunststück war nun, die Systeme so schnell wie möglich und mit möglichst geringem Risiko wieder hochzufahren. Es war ein Balanceakt zwischen Schnelligkeit und Sicherheit, da der Angreifer und seine Backdoors nach wie vor im System waren – dieses jedoch so wiederhergstellt werden sollte, wie es vor dem Angriff war. Wir mussten bei jeder Aktion abwägen, in welcher Reihenfolge wir am besten vorgehen und welches Risiko wir eingehen.", erinnert sich Panow.

„Es waren immer zwei Schritte vor und ein Schritt wieder zurück."

Um die Systeme in der Reihenfolge der Business-Priorität vorsichtig wieder hochzufahren, haben die Experten die Internetverbindung zunächst vollständig geblockt. Alle Zugriffe wurden anschließend gründlich kontrolliert, um mit Whitelists zu arbeiten. Zusätzlich wurde eine clientbasierte Software eingesetzt, die jede Maschine hinsichtlich ihrer Verhaltensmuster und Prozesse analysiert. So konnte beispielsweise festgestellt werden, wenn ein Server über einen unüblichen Port mit einem anderen Gerät kommuniziert.

Schließlich wurden die einzelnen Maschinen aus dem Backup wiederhergestellt, da dies deutlich weniger Zeit in Anspruch nahm, als jedes Gerät einzeln zu entschlüsseln. „Unsere Herausforderung war ganz klar, dass wir im laufenden Betrieb am offenen Herzen die Sicherheit optimieren und garantieren mussten. Um den Überblick zu behalten, haben wir die Kanban-Methode angewandt, bei der die einzelnen durchlaufenen Prozessschritte der Systeme auf Karten visualisiert werden."

netcos GmbH
Richard-Strauß-Straße 71, 81679 München
Tel.: +49 (89) 45 22 16-0
ww.netcos.de

Ganzheitliche IT-Sicherheit – mehr als Firewall und Antivirus

Während des etwa vierwöchigen Prozesses wurde dem Experten-Team die Relevanz bestätigt, den internen Netzwerktraffic zu überwachen. Denn nur in einem sichtbaren Netzwerk lässt sich rechtzeitig feststellen, ob sich ein Angreifer bereits im System bewegt. „Man muss möglichst früh erkennen, ob jemand durch die eigenen Flure streicht und nach offenen Bürotüren schaut.“, erklärt Panow. „Wir konnten so beispielsweise erkennen, dass ein Rechner mit einem command and control-Server in Russland kommuniziert hat – und haben diesen direkt wieder offline genommen.“ Zudem solle durch eine Netzwerksegmentierung vermieden werden, dass sich z.B. alle Clients und Server im gleichen IP-Adress-Segment befinden.

Darüber hinaus wurde deutlich, dass eine saubere IT-Dokumentation unabdingbar ist. Hierzu gehört einerseits eine genaue Definition der Prozesse sowie der Reihenfolge, in der im Krisenfall vorgegangen werden muss. Zusätzlich ist ein gepflegtes Active Directory ein Muss, um im Restore-Fall einen Überblick der Zuordnung der User zu verschiedenen Abteilungen, dessen Kontaktdaten und Berechtigungsstufen zu erhalten. Hilfreich ist es auch, die Switch- und Firewall-Regelungen zu dokumentieren und darauf aufbauend eine Kommunikationsmatrix zu erstellen. Um die vollständige Dokumentation im Ernstfall zur Verfügung zu haben, sollte diese möglichst außerhalb des eigenen Systems abgelegt werden.

„Uns wurde erneut bewusst, dass ein ganzheitliches Sicherheitskonzept weit über das hinausgeht, was man normalerweise als IT-Dienstleister mit Firewall und Antivirus unter IT-Security versteht. Man muss sich jeden sicherheitskritischen Aspekt in der IT-Infrastruktur genau anschauen und mit dem Kunden detailliert darüber sprechen.“, resümiert Panow.

Dazu zählt neben dem sichtbaren Netzwerktraffic sowie der sauberen IT-Dokumentation in erster Linie das Backup. Wenn beispielsweise durch eine Zwei-Faktor-Authentifizierung oder andere Maßnahmen sichergestellt ist, dass die Datensicherung nicht angegriffen werden kann, haben Cyber-Attacken eine deutlich geringere Chance auf Erfolg. „Über Jahre hinweg haben Kriminelle gute Umsätze gemacht. Diese sind jedoch plötzlich eingebrochen, weil Unternehmen ein Bacup hatten und nicht auf Lösegeldforderungen eingehen mussten. Jetzt gehen Hacker erst auf die Datensicherung los, bevor sie alles andere verschlüsseln.“, erklärt netcos Geschäftsführer Stanislaw Panow.

Es bedarf also einer Überprüfung, mit welchen Mitteln das Backup potenziell durch wen gelöscht werden könnte. Um im Krisenfall möglichst effizient vorzugehen, sollte zudem bereits bei der Datensicherung priorisiert und die Backupsätze hinsichtlich ihrer Relevanz für die Business Continuity segmentiert werden. Zusätzlich ist es ratsam, ein Anti-Malware-Schutz in das Backup zu integrieren, damit im Ernstfall kein infiziertes System zurückgespielt wird. „Aber da arbeiten die Hersteller gerade erst dran.“

Um das Sicherheitsniveau ihrer Kunden möglichst hoch zu halten, arbeitet die netcos GmbH zudem mit detailliertem Whitelisting. Hierbei wird genau definiert, welche Abteilungen wann und warum Zugang zum Internet und spezifischen Websites benötigen. Zusätzlich wird darauf geachtet, welche Mitarbeiter einen Laptop für den Außendienst erhalten und welche Clients über einen offenen USB-Port verfügen müssen. Die Passwortverwaltung spielt außerdem eine wichtige Rolle im Sicherheitskonzept.

netcos GmbH
Richard-Strauß-Straße 71, 81679 München
Tel.: +49 (89) 45 22 16-0
ww.netcos.de

„Es ist nur eine Frage der Zeit, bis ein Hacker die Admin-Passwörter herausfindet – und wenn er sie hat, kann er alles machen." Deswegen sei es besonders wichtig, die Privileged Accounts zu schützen, indem man auf generische Accounts verzichtet und eine Zwei-Faktor-Authentifizierung einsetzt.

Zusätzlich betont netcos Geschäftsführer Stanislaw Panow, dass die User Awareness einen unmittelbaren Anteil zur IT-Sicherheit beiträgt. Denn der Enduser sei oft derjenige, mit dessen „Unterstützung" ein Angreifer in das System hineinkommt. Hier alle Nutzer durch entsprechende Schulungen zu sensibilisieren, sei zielführend.

Zum Unternehmen

netcos GmbH

IT-Dienstleister in München
gegründet 2002
aktuell 18 Mitarbeiter
Geschäftsführer: Stanislaw Panow
Schwerpunkte: Managed Services,
IT-Betrieb & IT-Beratung

„Die Gartenzäune müssen hoch sein"

Das betroffene Unternehmen hat alle relevanten Aspekte des ganzheitlichen Sicherheitskonzeptes erneut detailliert geprüft und auf ein sehr hohes Niveau gebracht. „Denn wenn so etwas ein zweites Mal passiert, ist die Firma weg vom Markt. Den Betrag des verursachten Schadens hat man in der Regel nicht auf der hohen Kante.", ist sich Panow sicher. Doch wenn das Unternehmen sich nach dem Angriff vollständig erholt habe, sei es seinen Mitbewerbern, die ein solches Fiasko noch nicht durchlaufen haben, meilenweit voraus.

„Angegriffen wird jeder früher oder später. Die Frage ist nur, wie hoch die Hürden sind. Ich benutze gerne die Metapher der Gartenzäune: Einbrecher gehen dort zuerst rein, wo niedrige, brüchige Zäune sind. Bei unserem Kunden haben wir jetzt eine drei Meter hohe Mauer inklusive Stacheldraht errichtet, wo man mehr als nur eine Leiter benötigt, um in den Vorgarten zu gelangen."

Bei seinen weiteren Kunden setzt Stanislaw Panow ebenfalls auf höchste Sicherheit, denn der Schutz vor Eindringlingen wird in Zukunft immer relevanter. „Das ist eine riesige Industrie geworden mit Milliardenumsätzen, die wieder in ausgeklügelte Maßnahmen und Angriffsmethoden reinvestiert werden."

Der zunehmenden Gefahren durch Cyberkriminalität sind sich netcos Kunden dank der Medienberichterstattung durchaus bewusst. Die Erfahrungen, die das Systemhaus zu berichten hat, nehmen viele jetzt zum Anlass, um das Projekt IT-Sicherheit endgültig anzustoßen. „Ich habe vor dem Krisenfall aus der Theorie gesprochen und beispielsweise Statistiken angeführt, wenn ich IT-Security beim Kunden adressieren wollte.

Jetzt hört mir mein Gegenüber ganz anders zu, weil er merkt, dass wir den Ernstfall live miterlebt haben und wissen, wie so etwas ablaufen kann." Gemeinsam feilen sie nun an Plänen, Mannschaften und Infrastrukturen für den Notfall sowie an Organisation und Kommunikationskanälen, um im Krisenfall bestens gerüstet zu sein.

netcos GmbH
Richard-Strauß-Straße 71, 81679 München
Tel.: +49 (89) 45 22 16-0
ww.netcos.de

Ganzheitliche IT-Sicherheit – mehr als Firewall und Antivirus

Für Unternehmen ist es zunehmend eine Herausforderung, den komplexen Sicherheitsanforderungen alleine gerecht zu werden.

Als Anbieter von Managed Security Services solle man laut Panow die Wahrscheinlichkeit eines Angriffs beim Kunden nicht beschönigen. Insbesondere diejenigen Unternehmen werden gerne von Cyberkriminellen anvisiert, die erfolgreich am Markt agieren, ein hohes Umsatzwachstum vorweisen und deren Organisationen schnell gewachsen sind.

Zielscheibe sind ebenfalls inhabergeführte Firmen, da diese dank kurzer Entscheidungswege im Ernstfall schnell zahlungsfähig sind.

Als dritte Gruppe kommen zudem Organisationen in Frage, die von IT besonders abhängig sind, jedoch eine sehr ausgelastete IT-Abteilung haben. „Wir reden von Digitalisierung, IoT und so weiter – aber wer setzt das Ganze um? Das sind die internen IT-Abteilungen. Und die haben jetzt schon viel zu tun. Das Thema IT-Security geht dann völlig unter."

Systemhaussicherheit nicht außer Acht lassen

Seinen Systemhauskollegen, die ihren Kunden Managed Security Services anbieten, rät Stanislaw Panow, nicht alleine auf die Technologien zu setzen. Es sei zusätzlich wichtig, sich intensiv mit der IT-Infrastruktur inklusive der dahinterstehenden Prozesse auseinander zu setzen und gemeinsam mit dem Kunden mögliche Angriffsszenarien durchzugehen – um schließlich alle relevanten Sicherheitsmaßnahmen zu treffen.

„Doch was bringt die höchste Schutzmauer beim Kunden, wenn der Gartenzaun des Systemhauses alt und wackelig ist? Man muss schließlich nicht den Berg angreifen, wenn man sich auch den Propheten vornehmen kann."

Stanislaw Panow

Geschäftsführer
netcos GmbH

netcos GmbH
Richard-Strauß-Straße 71, 81679 München
Tel.: +49 (89) 45 22 16-0
ww.netcos.de

Cyber Defense Service

Der virtuelle Abwehrschirm für Ihr Unternehmen

Sie möchten Ihre Unternehmens-IT sicher und noch effizienter machen?
Sie haben keine eigene IT-Abteilung und möchten sich gegen Cyberangriffe wappnen?

- Einfache Integration und schneller Einsatz
- Managed Service ohne zusätzlich interne Ressourcen – weder personell, noch technisch
- Klare und einfache Handlungsanweisungen
- Sensibler Umgang mit Unternehmensdaten
- Einhaltung deutscher und europäischer Technologie- und Compliance-Standards
- Erfüllung von Anforderungen an IT-Sicherheit und Risikomanagement

Vielschichtige Sicherheits-konzepte sind gefragt

Bereiten Sie sich auf einen möglichen Ernstfall mit den folgenden Tipps vor:

1. **Internen Netzwerktraffic überwachen**
   Nur in einem gut überwachten Netzwerk lässt sich rechtzeitig feststellen, ob sich ein Angreifer bereits im Netz bewegt.

2. **Netzwerk segmentieren**
   Clients und Server sollten sich in unterschiedlichen IP-Adress-Segmenten befinden.

3. **IT gut dokumentieren & Notfallplan erstellen**
   Hierzu gehört einerseits eine gute Dokumentation der IT-Systeme, aber auch die Definition der Notfall-Prozesse sowie der Reihenfolge, in der im Krisenfall die Systeme wieder in Betrieb genommen werden sollen. Diese Dokumentation sollte sich außerhalb des Unternehmensnetzwerks befinden.

4. **Backup – immer gut gesichert!**
   Das Backup muss gegen Manipulation oder Zerstörung geschützt werden. Zum Beispiel durch eine Zwei-Faktor Authentifizierung oder durch ein “Air Gap”, in dem die Datenträger mit dem Backup nur durch einen manuellen Eingriff verfügbar gemacht werden können.