Ausgabe 01/17

23. Januar 2017

Ausgabe 01 / 17

IT-Security

Vermeiden von Angriffen

GSG Global Service Group GmbH
EDV- und IT-Management

Themen in dieser Ausgabe:

- **Angriffe auf Unternehmen**
- **Wer trägt die Verantwortung?**
- **GSG Security Framework**

In dieser Ausgabe: Innenseite

Angriffe auf Unternehmen

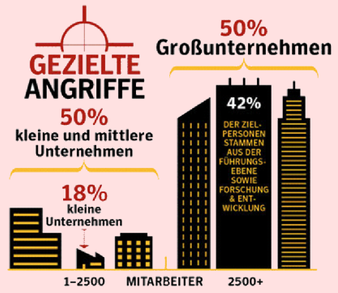
Angriffe auf Unternehmen werden häufiger, in zeitlich kürzeren Abständen und immer professioneller durchgeführt. Dabei ist zunehmend der Mittelstand im Visier der Angreifer: Über die Hälfte der Attacken richtet sich gegen Unternehmen mit weniger als 2.500 Mitarbeitern, knapp 20% sogar gegen Firmen mit weniger als 250 Beschäftigten.

Ging es den Hackern vor ein paar Jahren noch um Ruhm, Anerkennung und Befriedigung eines gewissen Spieltriebs, werden heute Datenklau und Sabotage über einen Dienstleister beauftragt, z.B. von Ihrem härtesten Konkurrenten. Der Schwarzmarkt im Darknet boomt.

Wussten Sie eigentlich, dass Sie einen Verschlüsselungstrojaner mit Hotlinesupport bereits ab 99€ kaufen können? Auch Kreditkarten-Accounts oder ganze Botnetze lassen sich heute bequem über Einkaufsportale in einem isolierten Bereich des Internets erwerben.

Wenn Sie heute angegriffen werden, wüssten Sie was zu tun ist?

Wissen Sie, welche Auswirkungen ein IT-Angriff auf Ihr Unternehmen hat? Wie hoch der finanzielle Verlust sein wird, ganz zu schweigen von Ihrem Image-Schaden?



Wir bieten einen kompletten Security-Service, von der Risikoanalyse über Penetrationstests bis zur Umsetzung von entsprechenden Maßnahmen und Unterstützung im Ernstfall.

Auch forensische Beweissicherung zur Feststellung des Täters nach einem Angriff gehören zu unserem Portfolio.

Wer trägt die Verantwortung?

Wer ist für ein angemessenes Sicherheitsniveau im Unternehmen verantwortlich? Ganz einfach: **Die Geschäftsleitung**.

Glauben Sie nicht? Die Rechtslage ist eindeutig und lässt sich aus verschiedenen Gesetzen und Richtlinien ableiten. Beispiele? Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) fordert ein Risikomanagement für Kapitalgesellschaften, das Aktiengesetz legt fest, dass ein Vorstand persönlich haftet, wenn Risiken nicht rechtzeitig erkannt und angemessen überwacht werden und dem Geschäftsführer einer GmbH wird durch das GmbH-Gesetz eine entsprechende Sorgfaltspflicht auferlegt.

Fallen Sie nicht darauf rein

Gefahrenpotential Mensch

Das größte Risiko für die Unternehmenssicherheit ist der Mitarbeiter. Jeder einzelne muss deshalb entsprechend sensibilisiert und geschult sein. Bei Angriffen über das sogenannte „Social Engineering“ versuchen Kriminelle, den Menschen und dessen „Schwachstellen“ mit unterschiedlichen Tricks und speziellen Techniken zu manipulieren und so an vertrauliche Informationen zu gelangen, sich Zugang zu internen IT-Systemen zu verschaffen oder direkt unzulässige Zahlungen anweisen zu lassen. Beim Social Engineering werden positive menschliche Eigenschaften, wie z.B. Hilfsbereitschaft, Vertrauen, Kollegialität oder Respekt in Autoritäten ausgenutzt. Durch plausibel klingende Geschichten und passende Rahmenbedingungen sowie den Überrumpelungseffekt können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln.

Auch ergeben sich Gefahren und Risiken, wenn Mitarbeiter das Unternehmen verlassen, beim Auslagern von Prozessen oder dem Einsatz von Fremdpersonal. Verlieren Sie hier nicht die Kontrolle über Ihr Firmen-Knowhow.

Um alle Sicherheitsaspekte des täglichen Berufsleben lückenlos abdecken zu können, muss Sicherheit im Unternehmen „(vor)gelebt“ werden. Jeder Mitarbeiter muss ein Grundverständnis für Informationssicherheit haben und „typische Maschen“ kennen, um Gefahren richtig einschätzen zu können.

Kostenreduzierung

zufriedene Mitarbeiter

vereinfachte IT

Schutz vertraulicher Daten

BYOD — Kontrolle AD?

Fast jeder verfügt heutzutage privat über ein Smartphone und/ oder Tablet und setzt diese oft auch für berufliche Zwecke ein. Markstudien bescheinigen sogar eine positive Unternehmensentwicklung, wenn Mitarbeiter ihre Privatgeräte beruflich nutzen (ByoD = Bring your own Device).

Dabei entstehen aber auch Probleme: Es ist nicht nur die Vielfalt der wireless Geräte, die in einem sonst klar beherrschbaren physikalischen Netzwerk kontrolliert werden muss, sondern vor allem die Einhaltung der Firmen Compliance. Weitere Herausforderungen sind die Sicherheit und die Verwaltung der Geräte, die Berücksichtigung der Netzwerklast und die Administration und der Support im Fehlerfall.

Grundvoraussetzung ist natürlich eine gute Planung, aber ohne die entsprechenden Werkzeuge lässt sich Sicherheit nicht realisieren.

Wir zeigen Ihnen, wie nicht nur die mobilen Geräte, sondern alle *Endgeräte* innerhalb Ihres Netzwerkes umfassend und effizient verwaltet werden.

Phantastische Aussichten.

Wieder beruhigt schlafen können

Risikomanagement

Risikomanagement ist keine lästige Pflicht, sondern eine Chance, IT-Prozesse zu optimieren und das Sicherheitsniveau zu erhöhen. Schwachstellen erkennen, das Risiko minimieren, die Bedrohung erfassen und den Angriff bewerten. Das ist Risikomanagement in Kurzform— im Prinzip ganz einfach. Aber was bedeutet dies genau?

Schwachstellen werden z.B. mittels Penetrationstests ermittelt, möglichst transparent und natürlich unter Einhaltung rechtlicher Vorgaben. Die Ergebnisse aus Bedrohungs– und Risikoanalyse zeigen die konkreten Gefahren auf. Unter wirtschaftlichen und organisatorischen Aspekten wird festgelegt, welche Abwehr-Maßnahmen für Ihr Unternehmen erforderlich und sinnvoll sind. Diese werden in einem Sicherheitsregelwerk erfasst und praktisch umgesetzt.

Mit diesen Maßnahmen steigern Sie das Vertrauen von Geschäftspartnern und Banken in Ihre Sicherheit nachhaltig.

Bleiben Sie stressfrei.

Das digitale Bollwerk

Sowohl die Zahl der zielgerichteten als auch die der automatisierten und damit letzlich zufälligen Angriffe auf Firmennetzwerke steigt enorm.

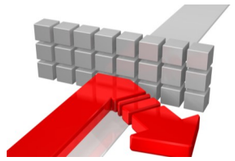
Es ist mittlerweile unumgänglich, Firewall-Appliances einzusetzen, welche als digitale Bollwerke einer Vielzahl von Gefahren aus dem Internet stand halten und somit die erste Schutzlinie des Unternehmens darstellen.

Es gibt für jede Unternehmensgröße angepasste Firewall-Appliances, die mit intelligenten Sicherheitssystemen Angreifer isolieren, den gesamten Netzwerkverkehr auf Schadsoftware prüfen, Eindringungsversuche in Ihr Netzwerk verhindern und gegebenenfalls automatisch Gegenmaßnahmen einleiten.

Und über das VPN-Gatewaymodul können Mitarbeiter im Außendienst oder im Home-Office über eine gesicherte Verbindung auf freigegebene Ressourcen ihres Unternehmensnetzwerkes sicher zugreifen.

Die Kombination einer Firewall-Appliance mit intelligentem Netzwerkmanagement ermöglicht es so, kritische Netzwerkbereiche zu segmentieren und zu isolieren, um Ihre Daten und Systeme noch effektiver vor Angriffen von Innen und Außen zu schützen.

Dabei ist es nicht angemessen und notwendig, jedes Unternehmen gleich wie Fort Knox zu sichern. Wir helfen Ihnen, zu erkennen, wieviel Sicherheit Sie wirklich brauchen!



Hier kommst Du nicht rein!

Log-Management ist Pflicht

Wenn ein Security-Vorfall entdeckt wird, geschieht dies meist aus Zufall und oft viel zu spät. Noch schlimmer: Viele erfolgreiche Security-Vorfälle werden erst gar nicht erkannt und sind somit eine permanente geheime Bedrohung.

Die manuelle Suche nach Hinweisen auf einen Sicherheitsvorfall dauert wegen der enorm gestiegenen Anzahl der erzeugten Logdateien ewig und ist sehr fehleranfällig.

Nutzen Sie besser die Stärke von Security-Intelligence-Systemen und analysieren Sie in Echtzeit und automatisiert die Log-Informationen in Ihren Netzwerken.

Schon während eines Angriffes erhalten Sie Informationen, um direkt Abwehrmaßnahmen einleiten zu können.

Schützen Sie Ihre Systeme mit intelligenten Automatismen und informieren Sie sich über die verständlich und anschaulich gestalteten Reports regelmäßig über Ihre aktuelle Sicherheitslage.

Über entsprechende Produkte (Splunk, SIEM, Q-Radar) informieren wir Sie gern und beachten dabei, was zu Ihnen und Ihrem Unternehmen am besten passt.

Die Frage ist nicht,

ob Sie gehackt worden sind,

die Frage ist,

wann Sie es merken!

Was, wenn der Ernstfall eintritt...?

Sind Sie bereits Opfer eines Hackerangriffes geworden oder wurden die Daten Ihres Unternehmens durch Ransomware verschlüsselt?

Ob Ihr Unternehmensauftritt im Internet durch eine Flut von DDOS Paketen tagelang nicht erreichbar ist oder der eigene Mitarbeiter Daten an Dritte verkauft: Sie brauchen dann die **IT-Forensik**.

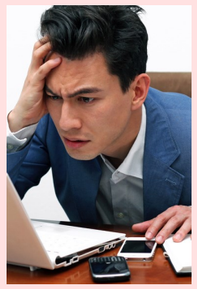
Wir unterstützen Sie im Ernstfall und führen die notwendige forensische Beweissicherung durch.

Unsere zertifizierte Forensik - abteilung analysiert die sichergestellten Geräte und Datenbestände auf Spuren, um die Übeltäter zu überführen.

Holen Sie sich die Kontrolle über Ihr Unternehmen zurück!

Viele Unternehmen wissen nicht, wie sie sich bei akuten IT-Sicherheitsvorfällen richtig verhalten und begehen in der Aufregung Fehler, die wichtige Datenspuren der Täter verwischen.

Lassen Sie sich daher **vorher** von uns über Maßnahmen beraten, die Sie im Ernstfall durchführen aber auch wie Sie und Ihre Mitarbeiter sich dann richtig verhalten sollten.



Wurden Sie gehackt?

... Was nun?

GSG Global Service Group GmbH
EDV- und IT-Management

Darmstädter Straße 53
D 64354 Reinheim

Telefon: (049) 6162 1051
Fax: (049) 6162 1055
E-Mail: gsg@gsg-edv.de

SIE FINDEN UNS AUCH IM WEB UNTER: WWW.GSG-EDV.DE

Weitere Informationen zu diesen Themen finden Sie auch bei unserem Partner-Unternehmen:

DR-THIELE.IT

GSG-Portfolio:

- **IT-Infrastruktur Administration und Wartung**
  - **Serversysteme**
  - **Netzwerke**
  - **Clientsysteme**
  - **Monitoring und Services**
- **Cloud-Provider und Managed-Services**
- **IT-Consulting**
  - **IT-Security**
  - **IT-Forensik**
- **Hard– und Software Handel**
- **Kunden-Schulung und Support**

GSG Security Framework

IT-Security kann nur dann vor Gefahren schützen, wenn Sie ganzheitlich und nach gewissen Vorgaben implementiert wird.

Vom Basisschutz bis hin zur Mitarbeiterschulung, von Social Engineering bis zu Penetrationstests, von Notfallmanagement über Schwachstellenanalyse bis hin zum Sicherheitskonzept bieten wir alle Möglichkeiten der Analyse und Umsetzung einer angepassten Sicherheitslösung. Entsprechend einzusetzende Produkte werden durch uns implementiert, angepasst und übergeben oder weiter betreut. Hierfür bieten wir auch cloudbasierte Lösungen an.

Digitale Beweissicherung und eine forensische Live– oder Post-Mortem Analyse Ihrer Geräte und Datenbestände nach einem Hackerangriff oder einer Kompromittierung gehören ebenso zu unseren Leistungen wie Hilfestellungen bei einer IT-Security Zertifizierung (z.B. nach VDS-3473)

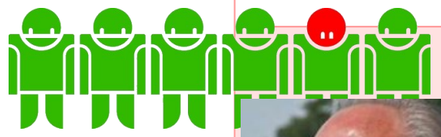
GSG kann auf eine lange Tradition von Partnerschaften zurück blicken, diese bilden ein ganz besonderes Potential bezüglich Reaktionszeiten und Support. Unsere (und damit auch Ihre) besonders wichtigen Partner auf dem Gebiet der IT-Security sind IBM, Microsoft, Securepoint, Sophos, GDATA und auch Kaspersky.

Profitieren Sie von unseren Erfahrungen und Fähigkeiten und lassen Sie uns Ihr Sicherheitsempfinden gemeinsam updaten, um zu objektiven und klar definierten Erkenntnissen zu gelangen, an welchen Stellen Ihre Sicherheit bereits ausreicht und wo gegebenenfalls Änderungen oder Nachbesserungen vorgenommen werden müssen.

Lassen Sie uns mit einem Gespräch beginnen.

Dr. Thiele IT-Beratung

Eine Kette ist nur so sicher, wie ihr schwächstes Glied



Ihr Dr. Frank H. Thiele

IT-Sachverständiger, Datenschutzexperte, IT-Sicherheitsbeauftragter und Vorstand des Kirchheimer-Kreises e.V.