
FOTOS: LAWRENZ

**Philippe Schaeffer (oben), Geschäftsführer der Bergisch Gladbacher Jester Secure iT GmbH, schlüpft regelmäßig in die Rolle eines Hackers – allerdings ganz legal im Auftrag von Unternehmen. So findet er Sicherheitslücken. Sebastian Feik (unten), Geschäftsführer der Bergisch Gladbacher legitimis GmbH, widmet sich vor allem dem Thema Datenschutz mit all seinen Facetten.**



**Wie ist die aktuelle Situation?** „Wir haben eine Bedrohungslage, die nicht ungefährlich ist", sagt Philippe Schaeffer, Mitgründer und Geschäftsführer des Bergisch Gladbacher Unternehmens **Jester Secure iT GmbH.** Zwar sei die Technik im Laufe der vergangenen Jahre immer besser geworden. „Jedoch gehen auch die Täter mit der Zeit und lassen sich ständig neue Methoden einfallen", sagt Schaeffer, der sich selbst als „Hacker – aber auf der guten Seite" bezeichnet. Es gebe seit Jahren ein „Wettrüsten", sagt Ralf Gogolin, Geschäftsführer der **HEGO Informationstechnologie GmbH.** „Der Angreifer ist immer der Schnellste. Man kann nur versuchen mitzuhalten." Was Gogolin und seine Mitarbeiter bei Neukunden zu sehen bekommen, sei zum Teil „wirklich erschreckend", sagt er. „Das ist so, als wenn man seine Haustür sperrangelweit offen stehen ließe", so Gogolin, der HEGO 1997 gemeinsam mit Jörg Hermanns gegründet hat. „Das ist dann eine Einladung für jeden Hacker." Und das in einer Zeit, wo man nicht einmal mehr selbst Programmierkenntnisse haben muss, um Schadsoftware zu verbreiten. „Die kann der Täter bequem über ansprechend gestaltete Internetseiten in Russland kaufen – ganz anonym, beispielsweise per Paysafe-Card, und direkt mit Update-Service", sagt Gogolin.

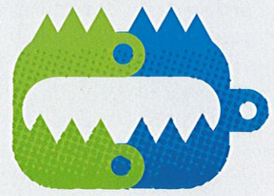
Ob ein Unternehmen – egal, ob Großkonzern oder mittelständisches Unternehmen – gut, schlecht oder gerade noch ausreichend in Sachen IT-Sicherheit aufgestellt ist, ist natürlich eine Definitionssache. Wenn sie eine prozentuale Einschätzung geben sollen, landen die verschiedenen IT-Experten aus dem Rheinisch-Bergischen Kreis jedoch alle in etwa bei dem gleichen Wert: Rund 80 Prozent seien schlecht aufgestellt. „Teilweise ist die Situation niederschmetternd, wenn man sich den Ist-Zustand bei Neukunden anschaut", sagt Sebastian Feik, Gründer und Geschäftsführer der Bergisch Gladbacher **legitimis gmbh** – einem Unternehmen, das sich vorwiegend dem Thema Datenschutz widmet. Wolfgang Straßer, der vor 13 Jahren – übrigens von der RBW begleitet – sein Unternehmen **@-yet GmbH** in Leichlingen gegründet hat, formuliert es bewusst drastisch: „Die Bedrohung ist da! Permanent und ständig!" 100 Prozent Sicherheit gebe es nicht, so Straßer. „Aber zehn bis 20 Prozent – in dem Bereich ist die Unternehmenssicherheit im Durchschnitt anzusiedeln – reichen definitiv nicht aus."

**Was sind konkrete Bedrohungen?** „Die Bedrohungsszenarien sind sehr vielfältig", sagt Robert Oevermann, Geschäftsführer der Bergisch Gladbacher Firma **OEVERMANN Networks GmbH.** Der Grund: Es gibt unterschiedlichste Hacker-Typen und verschiedenste Motivationslagen. Wolfgang Straßer: „Der eine handelt aus wirtschaftlichen Gründen – er will entweder Geld vom gehackten Unternehmen erpressen oder er verkauft erlangte Informationen; dann gibt es aber noch Hacker, die aus Rache oder aus ethischen Motiven handeln – oder ganz einfach, weil sie Spaß daran haben." Hinzu kommt: „Ohne funktionierende IT geht heutzutage kaum noch etwas", sagt Simon Rocholl, Geschäftsführer der Overather **smartworx Brewig / Rocholl GbR.** „Noch vor zehn Jahren war es oft kein großes Problem, wenn ein System ausgefallen ist, weil es meist eine nicht IT-basierte Alternative gab. Heute ist alles vernetzt. Ein gelungener Angriff an einer Stelle des Netzwerks kann schnell alles lahmlegen."

Ralf Gogolin sagt: „Man muss heutzutage viel mehr bedenken, es gibt viel mehr Möglichkeiten. Die komplette Unternehmenskommunikation hängt heute häufig daran – beispielsweise durch Telefonie über das Internet. Ein Virenangriff ist Stand der 1980er-Jahre. Heute läuft ein Angriff über völlig andere Wege. Darum reicht es auch nicht, wenn ein Unternehmen es damit bewenden lässt, einen Virenscanner zu kaufen. Man kann beispielsweise Trojaner auf eine Webseite legen, ohne dass der Betreiber das merkt, in Netzwerke eindringen oder Schadsoftware über die Schnittstellen des Arbeitsplatzrechners einschleusen."

Eine weitere Herausforderung ist, dass der Schutz heutzutage nicht mehr an den Wänden des Firmensitzes endet: „Das Büro ist heute immer mit dabei – durch Tablets und Smartphones. Damit werden häufig öffentliche WLAN-Verbindungen – auch im Ausland – genutzt", sagt Straßer. „Dadurch entstehen völlig neue Bedrohungslagen für Unternehmen. Oft sind Smartphones, Tablets oder Cloud-Lösungen bereits implementiert, bevor die IT-Sicherheitsverantwortlichen und Datenschützer sich um deren Absicherung kümmern konnten."

Ganz konkret werden einem Unternehmen die Gefahren bei einem „Penetration Test" aufgezeigt. Straßer: „Die Unternehmen werden dabei – ganz legal



*„Wer etwas Besonderes macht, ist interessant für Hacker; wer nichts Besonderes macht, wäre nicht mehr am Markt."*

RALF GOGOLIN

und mit der Geschäftsführung vertraglich vereinbart – angegriffen. Wir schauen: (Wie) Kommen wir rein? Merkt es die IT? Wir versuchen, uns Rechte zu erarbeiten bis hin zu Administratorenrechten. In 95 Prozent aller Fälle gelangen wir zum Admin-Level, ohne dass es die IT bemerkt – und das in viel zu schneller Zeit."

**Warum tun Unternehmen zu wenig?** Die Bedrohung ist also da – und wird offenbar stetig größer. Interessant ist da die Frage, warum sich viele Unternehmen – trotz vorhandener Möglichkeiten – verhältnismäßig wenig schützen. „Viele kommen erst zu uns, wenn bereits etwas passiert ist", sagt Simon Rocholl. „Bis zu diesem Zeitpunkt war IT-Sicherheit für die Unternehmen oft nur ein lästiges, abstraktes Thema." Ralf Gogolin sieht das ähnlich: „Es herrscht nach wie vor das Denken vor: ‚Uns wird es schon nicht treffen.'" Gerade bei kleineren Unternehmen komme häufig das Argument: „Wir sind doch viel zu uninteressant für einen Hacker."

Gogolin entkräftet dieses Argument: „Wer etwas Besonderes macht, ist interessant für Hacker; wer nichts Besonderes macht, wäre nicht mehr am Markt." Viele schieben die Problematik laut Sebastian Feik gedanklich ganz weit weg. „Man nimmt erst Anteil daran, wenn es näher rückt. Wenn befreundete Unternehmen betroffen sind oder wenn ein Fall in der eigenen Stadt passiert." Viele Fälle werden jedoch nicht bekannt. Denn logischerweise hat kein Unternehmen ein Interesse daran, so etwas zu kommunizieren. „Viele wissen aber überhaupt nicht, dass sie längst selbst betroffen waren oder sind", sagt Feik, „weil häufig ein Monitoring fehlt."

Zum fehlenden Bewusstsein kommt laut Wolfgang Straßer ein weiterer Faktor: „Es kostet halt Geld", sagt er. „Und man bekommt dafür nichts Greifbares."

**Was müssen Unternehmen für Sicherheit ausgeben?** „Eine konkrete Summe, wie viel ein Unternehmen in seine IT-Sicherheit investieren sollte, kann man pauschal nicht nennen", sagt Ralf Gogolin. Dafür seien Strukturen und die Anforderungen an die Sicherheit zu verschieden. „In etwa sollte der Preis für die Sicherheit dem Preis der Infrastruktur entsprechen", gibt Gogolin einen ungefähren Richtwert. „Wir beraten, was aus unserer Sicht zwingend notwendig ist und was nicht." Simon Rocholl formuliert es so: „Wir zeigen zunächst einmal neutral die Risiken auf und entwickeln eine bedarfsgerechte Lösung. Man muss ja nicht mit Kanonen auf Spatzen schießen." Philippe Schaeffer ergänzt: „IT-Sicherheit muss nicht teuer sein. Man muss es nur richtig machen." Es müsse auch nicht zwingend jede Sicherheitslücke geschlossen werden. „Es ist ein Abwägungsprozess, den der Unternehmer treffen muss – eine Abwägung von Kosten und Risiken." Aus seiner Erfahrung heraus sagt Ralf Gogolin: „Die Bereitschaft, das Risiko einzugehen, ist hoch. Die Bereitschaft, für IT-Sicherheit Geld auszugeben, ist wenig verbreitet." Einen Rat gibt Gogolin: „Es bringt nichts, wenn man einmalig eine große Summe investiert, dann aber monatelang nichts tut. Dann ist man schnell wieder bei null."

Während die Unternehmen in vielerlei Hinsicht frei entscheiden können, wie viel sie investieren wollen und wie viel Risiko sie eingehen wollen, macht der Gesetzgeber auch immer mehr Vorschriften. So sind Unternehmen verpflichtet, Datenschutz zu betreiben. Das gilt auch für kleine Unternehmen, die keinen Datenschutzbeauftragten (das ist erst dann verpflichtend, wenn mehr als neun Personen mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind) bestellen müssen. „Ein Datenschutzbeauftragter muss aber nicht beim Unternehmen angestellt sein, man kann sich diese Leistung auch extern einkaufen", sagt Sebastian Feik.

**Warum sollten/müssen Unternehmen etwas tun?** Die Antwort auf diese Frage ist eindeutig: Zwar kostet IT-Sicherheit Geld, aber der Schaden durch Hacking oder Datendiebstahl kann immens sein. „Wir haben jedoch schon Fälle erlebt, zu denen wir leider nicht präventiv, sondern erst als Feuerwehr gerufen wurden, bei denen der Schaden in die Hunderttausende ging", sagt Simon Rocholl. Wobei es schwer sei, den Schaden klar zu beziffern. „Wie hoch ist der Schaden, wenn ein Konkurrent plötzlich Ihr gesamtes Wissen und dazu noch alle Kundenkontakte hat?", gibt Robert Oevermann zu bedenken. Und: Durch einen Hackerangriff kann schnell ein immenser Imageschaden entstehen. „Stellen Sie sich vor, dass plötzlich in Ihrem Namen Tausende Mails mit Schadsoftware verschickt werden", nennt Ralf Gogolin ein Beispiel, das in diesem Fall zudem als Verstoß gegen das Bundesdatenschutzgesetz (BDSG) geahndet werden kann, selbst wenn der Betroffene überhaupt nicht weiß, dass sein Server Schadsoftware versendet.

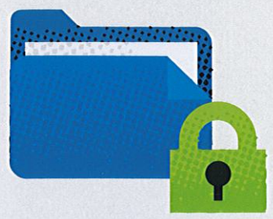


FOTO: LAWRENZ

**Wolfgang Straßer hat vor 13 Jahren das Unternehmen @-yet GmbH in Leichlingen gegründet. Firmensitz ist mittlerweile das historische Schloss Eicherhof. Im Laufe der Jahre hat Straßer mitverfolgt, wie sich Angriffe von Hackern und Cyberkriminalität verändert haben. Seine Einschätzung lautet: „Die Bedrohung ist da! Permanent und ständig!"**

Und Verstöße gegen das BDSG können teuer werden. Bei vorsätzlichen oder fahrlässigen Verstößen droht ein Bußgeld von bis zu 50.000 Euro, bei schwerwiegenden vorsätzlichen Verstößen gar eine Freiheitsstrafe von bis zu zwei Jahren. Entsteht dem von einem Datenschutzverstoß Betroffenen ein materieller oder immaterieller Schaden, so steht ihm zudem die Geltendmachung von Schadensersatz oder Schmerzensgeld zu.

Durch das im Juni verabschiedete IT-Sicherheitsgesetz werden die Betreiber und Zulieferer besonders gefährdeter Infrastrukturen (sogenannter kritischer Infrastrukturen) wie Energie- oder Telekommunikationsnetze verpflichtet, ihre Netze besser vor Hackerangriffen zu schützen. Neben der dann obligatorischen Meldung von IT-Sicherheitsvorfällen werden Mindeststandards für die IT-Sicherheit bei den Betreibern solcher IT-Infrastrukturen branchenweit festgelegt.

**Was können Unternehmen tun?** Es gibt keine universell anwendbaren Checklisten. Straßer: „Wir haben so etwas zwar für den internen Gebrauch – die sind aber 20 Seiten dick. Nicht alles gilt für jedes Unternehmen bzw. jede IT-Infrastruktur. Das ist alles sehr individuell."

Dennoch gibt es einige grundsätzliche Tipps für Unternehmen. Wichtig sei es, sagt Robert Oevermann, ein funktionierendes Back-up zu haben. Dabei sollte man sich nicht darauf verlassen, dass das Back-up auch wirklich erzeugt wird, nur weil das System es anzeigt. „Wir werden immer wieder zu Neukunden gerufen, die sich sicher waren, dass das letzte Back-up 24 Stunden her ist, in Wirklichkeit ist es aber mehrere Monate alt, weil es irgendeinen technischen oder menschlichen Fehler gab." Oevermann: „Außerdem sollte man sich darüber bewusst werden, wo ein Angriff besonders wehtun würde." Was ist die Existenzgrundlage, was das wichtigste Kapital des Unternehmens? Womit kann man Abläufe lahmlegen? Ralf Gogolin nennt ein Beispiel, das zeigt, dass es auch ungewöhnliche Dinge sein können: „Wenn Abläufe in einem Unternehmen, wie Frachtpapiere eines Logistikunternehmens, von einem Nadeldrucker abhängen, dann ist dieses Gerät eine sehr sensible Stelle im Unternehmen, von der ganze Prozessabläufe abhängen können. Versuchen Sie mal, spontan einen Ersatz-Nadeldrucker irgendwo zu bekommen." Philippe Schaeffer: „Die Zugangswege sind auf den ersten Blick ungewöhnlich: Telefonanlagen können häufig in einen Wartungsmodus versetzt werden, das Passwort ist meist das werkseitig eingestellte – und schon sind wir im Netzwerk." Auch moderne Heizungsanlagen oder Druckerstraßen haben übrigens häufig Wartungszugänge.

Weniger ausgefallen, aber trotzdem immer relevanter, ist die Tatsache, dass Unternehmen immer mehr von der Funk-

tionsfähigkeit des Internets abhängig sind. „Auch hier kann durch Redundanz mit zwei Leitungen von zwei Internet-Providern präventiv vorgesorgt werden", rät Gogolin.

Laut Schaeffer ist es wichtig, sich nicht nur punktuell, sondern kontinuierlich um seine IT zu kümmern. „Wer kontinuierlich die Fehler- und Problemmeldungen, die das System speichert, auswertet und zudem alle sicherheitsrelevanten Updates durchführt, hat schon etwas ganz Wichtiges getan." Simon Rocholl: „Wenn man heutzutage beispielsweise noch Windows XP nutzt, dann öffnet man Tür und Tor für Angriffe." Denn: „Sicherheitsupdates gibt es hier nicht mehr." Straßer ergänzt: „Alle Systeme sollten natürlich auf dem neuesten Stand und die Firewall richtig eingestellt sein."

Ein weiterer Punkt: Kennwörter. Hier gibt es unterschiedliche Ansätze. Wie lang muss ein Kennwort sein? Muss es Sonderzeichen enthalten? Philippe Schaeffer: „Die meisten Kennwort-Richtlinien sind aus meiner Sicht kontraproduktiv. Ein Kennwort muss man zum Beispiel nur häufig ändern, wenn man es für verschiedene Accounts verwendet. Sobald ein Kennwort mehrfach benutzt wird, ist das schlecht, egal, wie viele Sonderzeichen darin vorkommen." Sein Rat: „Am besten ganze Sätze mit bewusst falsch geschriebenen und/oder individuellen Worten verwenden, die nicht im Duden stehen. Und lieber ein Kennwort notieren, als es mehrfach zu verwenden."

Neben allen technischen Vorkehrungen darf man eines nicht vergessen: den Faktor Mensch. „Der ist nämlich nach wie vor eine der größten Schwachstellen", sagt Wolfgang Straßer. „Wenn Mitarbeiter nicht wissen, warum sie etwas tun müssen – oder nicht tun dürfen, bringen viele Maßnahmen nichts. Darum spielt für uns die Schulung von Mitarbeitern eine große Rolle", sagt Sebastian Feik. „Wir erklären, dass bestimmte Maßnahmen notwendig sind – und warum sie notwendig sind." Robert Oevermann ergänzt: „Und die Mitarbeiter müssen bei Einführung neuer Programme und Geräte geschult werden." Gleiches gelte für neue Mitarbeiter. Umgekehrt sei es aber auch wichtig, sich Gedanken darüber zu machen, welche Abläufe notwendig sind, wenn Mitarbeiter das Unternehmen verlassen.

Grundsätzlich sollte man, so Straßer, misstrauisch sein, wenn man Mails von Leuten erhält, die man nicht kennt. Aber auch, wenn in Mails von Kontakten zu ungewöhnlichen Handlungen aufgefordert wird. „In dem Fall sollte man sich über ein anderes Medium, zum Beispiel das Telefon, vergewissern, dass alles seine Ordnung hat. Eine Nachfrage per E-Mail reicht logischerweise nicht aus, wenn der Account gehackt wurde."

Nach Einschätzung der IT-Experten gibt es also eine Bedrohungslage, die nicht nur auf Großstädte und Konzerne beschränkt ist. Es kann jeden treffen – auch das Ein-Mann-Unternehmen in Odenthal. In Panik verfallen muss man jedoch nicht. Denn: Man kann Vorkehrungen treffen und sich so schützen. Nur wer nichts tut, ist akut gefährdet.

**Philipp Nieländer**

## SPEZIALISTEN DER IT-SICHERHEIT

FOTOS: LAWRENZ

**@-yet GmbH**
Schloss Eicherhof
42799 Leichlingen
Tel.: +49 2175 16550
Fax: +49 2175 165511
www.add-yet.de

**Jester Secure iT GmbH**
Malteserweg 14
51465 Bergisch Gladbach
Tel.: +49 2202 983660
Fax: +49 2202 983666
www.jsec.de

**legitimis GmbH**
Dellbrücker Straße 116
51469 Bergisch Gladbach
Tel.: +49 2202 28941-0
Fax: +49 2202 28941-47
www.legitimis.com

**HEGO Informationstechnologie GmbH**
Telegrafenstraße 8
42929 Wermelskirchen
Tel.: +49 2196 88297-0
Fax: +49 2196 88297-23
www.hego-it.com

**smartworx Brewig / Rocholl GbR**
Zum Alten Wasserwerk 9
51491 Overath
Tel.: +49 2204 586120-0
Fax: +49 2204 586120-10
www.smartworx.de

**OEVERMANN Networks GmbH**
TechnologiePark, Haus 51
Friedrich-Ebert-Straße 75
51429 Bergisch Gladbach
Tel.: +49 2204 8444-00
Fax:+49 2204 8444-22
www.oevermann.de