

Link: <https://www.computerwoche.de/a/sicherheit-gibt-es-nur-im-gesamtpaket,2365238>

IT-Angriffe nehmen zu

Sicherheit gibt es nur im Gesamtpaket

Datum: 24.02.2011

Autor(en): Thomas Pelkmann

Spektakuläre Angriffe auf Firmennetze und -daten zeigen: Zahl und Qualität der Bedrohungen steigen dramatisch an. Die Gefahr lauert aber nicht nur außerhalb der Unternehmen; fahrlässige und mitunter gar böswillige Mitarbeiter verursachen ebenso große Schäden. Technische Abwehrmaßnahmen helfen da nur bedingt. Stattdessen sind ganzheitliche Konzepte gefragt, die vom gesamten Unternehmen getragen werden.

□

Foto:

Rund drei Viertel der deutschen Unternehmen haben eigenen Angaben zufolge schon einmal Erfahrung mit Angriffen auf die Unternehmens-IT gemacht, hat IDC in einer Umfrage herausgefunden. Es ist nicht unwahrscheinlich, dass auch das fehlende Viertel bereits Ziel strafatbewehrter Attacken geworden ist - und es einfach nicht gemerkt hat.

Zur Verschärfung des Problems tragen die **sozialen Netzwerke des Internet**¹ bei. Bei LinkedIn oder Facebook bewegen sich zunehmend - und oft von den Unternehmen gewollt - auch die eigenen Mitarbeiter, um ihre Firma dort zu repräsentieren. Schließlich ist die zunehmende Nutzung von **Cloud-Services**² ein neue potenzielle Gefahrenquelle: Firmendaten sind nun nicht mehr nur in internen Netzen gefährdet, sondern nun auch an Orten, die ein durchschnittlicher Cloud-Kunde in der Regel gar nicht kennt.



Nur wenige Länder verfolgen Verstöße gegen die IT-Sicherheit systematisch, meint Lynn-Kristin Thorenz, Director Consulting bei IDC Central Europe.

Bei fast der Hälfte der befragten Unternehmen haben die Angriffe zu Ausfällen in der IT und damit zu messbaren Schäden geführt. Immerhin bei einer von fünf Firmen waren Imageschäden und Vertrauensverluste bei den Kunden die Folge.

Dabei gibt es bei den technischen Vorkehrungen gegen Eindringlinge und Angreifer nur wenig zu meckern: Fast alle Unternehmen verfügen über einen IT-Grundschutz aus Virenschutzprogrammen, Spamfilter und Firewalls. Aber nicht nur an der Wirksamkeit dieser **Endpoint Security**³ äußern Experten Zweifel, weil sie im besten Falle Angriffe nur abwehren hilft, nicht aber von vorneherein verhindert. Vor allem scheitern solche Tools oft an den Mitarbeitern, die mit ihnen umgehen sollen. Halten die sich nicht an die Regeln, finden Angreifer reichlich Hintertüren über E-Mails und Tauschbörsen, um trotzdem einen Fuß in die Unternehmen setzen zu können. Dazu kommen Kollegen, die nicht fahrlässig Verluste durch Eindringlinge verursachen, sondern absichtlich: Nicht in der Zahl der Angriffe, aber in der Schadenssumme liegen solche Angriffe von innen deutlich vorne.

Druck durch Compliance und Rechtsvorschriften wächst

Stress für die Sicherheitsaktivitäten von Unternehmen drohen auch auf der regulativen Seite. Die Anforderungen an die Compliance nehmen zu und betreffen beispielsweise den höheren Schutz von Kunden- und Mitarbeiterdaten. Zwar gibt es bislang nur wenig Länder, in denen die Exekutive systematisch die Verstöße gegen Compliance-Vorschriften verfolgt, meint **Lynn-Kristin Thorenz, Director Consulting bei IDC Central Europe**⁴. Aber zum einen nehme die Zahl der Sanktionen dennoch zu, zum anderen stiege die Höhe der Strafzahlungen bei Verstößen empfindlich an.

Die zunehmenden Bedrohungen von innen und außen und der wachsende Druck von Gesetzgebung und Exekutive zwingen die Unternehmen, sich nicht nur reaktiv mit den Gefahren zu befassen, sondern strategisch, prophylaktisch, nachhaltig und als gesamtes Unternehmen.

Je größer das Unternehmen, desto eher gebe es solch ein strategisches Sicherheitsdenken, meint Peter Maucher, bei HP leitender Berater für Governance, **Compliance**⁵ und Informationssicherheit. Dort gebe es zudem oft bereits eigene Compliance- und Sicherheitsorganisationen, die über die Einhaltung der Sicherheitsregeln wachten. Bei mittelständischen und kleinen Unternehmen (KMU) sehe die Sache aber schon ganz anders aus. "Da ist das Thema in den Chefetagen noch nicht so richtig angekommen" meint Maucher. "Die denken immer noch, sie lebten in Deutschland auf einer Insel der Glückseligen"; wenn es jemanden treffe, dann immer den anderen.

Dabei sei gerade bei den **KMUs**⁶ für Angreifer richtig was zu holen: "Diese Unternehmen haben wahnsinnig viel Know-how und prägen mit ihren Patenten und Produktionsverfahren letztendlich unsere Volkswirtschaft mehr als die vergleichsweise wenigen Großunternehmen."

So pointiert sich der HP-Experte auch ausdrückt: Von einer pauschalen Bewertung der KMUs möchte Maucher nichts wissen: Wo IT nicht Kernkompetenz des Unternehmens sei, arbeiteten oft nur zwei bis acht Mitarbeiter daran, die IT-Infrastruktur am laufen zu halten. "Da gibt es keine Kapazitäten für großartige strategische Planungen."

Dazu komme, pflichtet IDC-Analysten Lynn-Kristin Thorenz bei, dass es bei Investitionen in die IT-Sicherheit schwer sei, über einen **Return-on-Invest (ROI)**⁷ zu diskutieren. "Solche Investitionen amortisieren sich nicht", so Thorenz. "Das ist wie bei einer Versicherung für den Fall, dass vielleicht irgendwann mal etwas passiert, und das kostet einfach Geld."

Mechanische Sicherheitsvorkehrungen reichen nicht aus

Bei allem Verständnis für die Nöte der kleinen und mittelständischen Unternehmen: "IT-Sicherheit", meint die IDC-Analystin in ihrer 2010 erschienenen **IT Security-Studie**⁸, "ist zunehmend eine ganzheitliche Aufgabe". Zwar stehe - gleichsam als Pflicht - die Technik im Vordergrund. Die Kür einer umfassenden Sicherheitsstrategie erfordere aber zudem auch "organisatorische Maßnahmen wie Unternehmens- und Nutzerrichtlinien sowie Zertifizierungen". Ist ja auch logisch: Wo potenziell die Mitarbeiter - ob bewusst oder unbewusst - die Urheber von Datenverlusten sind, sind rein mechanische Sicherheitsvorkehrungen wichtig, reichen aber nicht aus.



Ohne überzeugte Mitarbeiter lässt sich kein Sicherheitskonzept umsetzen, ist sich Peter Maucher sicher. Er ist bei HP leitender Berater für Governance, Compliance und Informationssicherheit.
Foto: HP, Peter Maucher

Zu allererst, da sind sich Lynn-Kristin Thorenz und Peter Maucher einig, gehe es darum, die **Awareness**⁹ für das Thema Sicherheit zu erhöhen. "Viele Mitarbeiter sind sich einfach nicht über die möglichen Gefahren bewusst", meint Thorenz. Hier gehe es also vor allem um Aufklärung sowie um die Vermittlung von verbindlichen Regeln und Umgangsformen.

Meistens empfänden die Mitarbeiter Sicherheitsregeln als lästige Pflicht, deren Erfüllung ihre Arbeit behindere und aufhalte. Solche Maßnahmen, so Thorenz, könnten aber nur greifen, "wenn die Sicherheitskonzepte auch gelebt werden". Die Sensibilisierung der Mitarbeiter sei unumgänglich, um einen wirksamen Schutz des Unternehmens zu gewährleisten. Hier sollte man vor allem auf die betriebswirtschaftlichen und rechtlichen Konsequenzen hinweisen, "auf überzogene Schreckensszenarien" aber verzichten, rät die IDC-Analystin.

Stattdessen müsse man, ergänzt Peter Maucher, die Mitarbeiter unbedingt davon überzeugen, dass nicht nur die Firma, sondern auch sie selbst von den Richtlinien profitierten, "sonst funktioniert es nicht". Wer etwa wisse, dass zum Beispiel auch die eigenen persönlichen Daten zum schützenswerten Gut gehören - Vertragsdaten, Gehaltsdaten, eventuell in den Personalakten auch Daten über Fehlverhalten oder Krankheiten - der werde sich viel nachhaltiger am Datenschutz beteiligen.

Zudem hat ein einfacheres Leben, wer sich an die Regeln hält: Die verbindlichen Vorschriften entlasten den Mitarbeiter davon, sich bei jeder Aktion neu Gedanken machen zu müssen, ob er sich gerade regelkonform verhält. "Und wenn sich herausstellt, dass die Regeln falsch oder unvollständig waren, dann war es nicht mein Fehler, wenn trotzdem mal was schief geht", erläutert HP-Sicherheitsexperte Maucher einen weiteren Vorteil verbindlicher Vorschriften.

Geschäftsleitung muss mitmachen

Zu einem ganzheitlichen Informationssicherheitskonzept gehört auch die Einbeziehung des gesamten Unternehmens außerhalb der IT. Das fängt bei der Geschäftsleitung an: Die muss die Sicherheit der Unternehmensdaten zur Führungsaufgabe machen und dafür sorgen, dass Regelwerke unternehmensweit aufgestellt und eingehalten werden. Das geht über die Fachabteilungen, in denen die Mitarbeiter Tag für Tag sitzen und mit den konkreten Problemen von richtigem Verhalten, **Datenschutz**¹⁰ und Abwehr von Angriffen konfrontiert werden. Das betrifft die Personalabteilungen in den Unternehmen, die sich in organisierter Form zum Beispiel mit der Schulung und der Weiterbildung von Mitarbeitern befassen. Und dazu gehören - da sind sich die Experten im Sinne eines ganzheitlichen Konzepts einig - eben auch Schulungen und Weiterbildungen speziell zur Informationssicherheit. Erst für den Rest, die technischen Maßnahmen, die Tools, die **Monitoring-Werkzeuge**¹¹, die Peter Maucher zufolge maximal 50 Prozent der Schutzmaßnahmen ausmachen, ist dann die IT-Abteilung zuständig.

Erfolgreiche Regeln brauchen Kontrolle

Mängel in der Informationssicherheit sind auch auf fehlende Sanktionen zurückzuführen. "Es gibt weder in Deutschland noch auf europäischer Ebene Institutionen die mit dem TÜV oder einer Wirtschaftsprüfung vergleichbar wären", sagt Lynn-Kristin Thorenz. Auch Peter Maucher beklagt die mangelnde Kontrolle bei der Einhaltung der gesetzlichen Vorschriften. Zudem seien die lange maximal zu erwartenden Strafzahlungen von 50.000 Euro viel zu gering gewesen. Da die Implementierung wirksamer Schutzmechanismen ein Vielfaches davon kostete, verzichteten die Unternehmen nach einer Wirtschaftlichkeitsrechnung früher einfach auf die Maßnahmen. "Das war billiger", so Maucher, der jedoch darauf hinweist, dass sich das mit der **Novelle des Bundesdatenschutzgesetzes 2009**¹² geändert habe. Nun seien bei Verstößen Strafen bis zu 300.000 Euro sowie Gewinnabschöpfungen möglich. Das würde Unternehmen wesentlich härter treffen. Allerdings: "Es schaut nach wie vor kaum jemand nach, ob die Vorschriften eingehalten werden", kritisiert Maucher.

Aber auch intern ist es wichtig, über Audits die Umsetzung von Regelwerken und Vorschriften zu kontrollieren. "IT-Sicherheit ist ein Prozess und kein Projekt mit definiertem Anfang und Ende", betont IDC-Analystin Thorenz. Es sei wichtig, diesen Prozess auf Dauer zu leben, und dazu gehöre es, regelmäßig über den Stand der Dinge und über Verbesserungsmöglichkeiten zu reden. Zudem sei es bedeutsam, die Einhaltung rechtlicher Vorschriften laufend zu beachten. Aus Sicht von IDC wird dieses Thema in der kommenden Zeit sogar an Wertigkeit noch zunehmen. "Neue gesetzliche Vorschriften, eine verschärfte Verfolgung von Verstößen, aber auch interne Regeln" verlangten es, sich gesetzeskonform zu verhalten. Das sei so komplex, dass viele Unternehmen gar nicht dazu in der Lage seien, diese Aufgaben alleine zu bewältigen. "Scheuen Sie sich nicht, hier auf externe Hilfe zurückzugreifen", rät Thorenz.

HP-Beratungsleistungen zur Informationssicherheit

Zum Beispiel auf die **Hilfe von HP**¹³: "Wir haben im Rahmen von Projekten über viele Jahre einen regelrechten Fundus von Tools und Dienstleistungen aufgebaut", erläutert Peter Maucher das Angebot von HP. "Wir nennen das unser ‚Awareness-Programm‘, mit dem wir in der Lage sind, je nach Kunde, Unternehmensgröße, internationaler Ausrichtung und Problemlage individuelle Maßnahmen zielgruppenorientiert durchzuführen."

Dazu gehören zum Beispiel Tools zur Risikoanalyse, auf verschiedene Zielgruppen zugeschnittene Schulungs- und Trainingsmaßnahmen, unterschiedliche Medienformen für die Vermittlung von Problemen und Lösungsansätzen sowie Werkzeuge für das Monitoring und Auditing der vereinbarten Sicherheitsmaßnahmen.

"Bei unserer Beratungsarbeit gehen wir auf die Unternehmenskultur und die vorhandenen Erfahrungen ein und suchen uns aus unserem Pool die individuell passenden Maßnahmen heraus", umschreibt Peter Maucher das Komplettangebot von HP. "Wir helfen Unternehmen beim Aufbau von Sicherheitsstrategien, beim Erstellen von Regelwerken, bei der Entwicklung unternehmensweit gültiger Sicherheitsprozesse, bei der Definition von Rollen und gegebenenfalls auch beim Aufbau einer Sicherheitsorganisation."

Mehr zum Thema

- **So bauen Sie ein erfolgreiches Sicherheitsoperationszentrum auf**¹⁴
- **Cyber-Bedrohungen und -Risiken besiegen**¹⁵
- **Nachweis des ROI für SIEM - Beispiele von der Front**¹⁶
- **Open Source Security Study**¹⁷

Eine hundertprozentige Sicherheit kann aber auch der in 15 Jahren Arbeit an der Informationssicherheit gestählte HP-Experte nicht bieten. "Was wir versprechen können, ist eine messbare Verbesserung der IT-Sicherheit. Zudem befähigen und schulen wir die Organisationen darin, alle Maßnahmen zur Informationssicherheit auf Dauer selber durchführen zu können." Verglichen mit der oft traurigen Realität in vielen deutschen Unternehmen wäre das schon eine ganze Menge.

Links im Artikel:

¹ <https://www.computerwoche.de/schwerpunkt/s/soziale-Netze.html>

² <https://www.computerwoche.de/management/cloud-computing/1881211/index4.html>

³ <https://www.computerwoche.de/schwerpunkt/e/Endpoint-Security.html>

⁴ http://www.idc.de/research/cv_thorenz.jsp

⁵ <https://www.computerwoche.de/schwerpunkt/c/Compliance.html>

- 6 <https://www.computerwoche.de/security/2362263/>
 - 7 <https://www.computerwoche.de/schwerpunkt/r/Return-on-Investment.html>
 - 8 http://www.idc.de/consulting/mc_itsecurity2010.jsp
 - 9 <https://www.computerwoche.de/mittelstand/1908847/>
 - 10 <https://www.computerwoche.de/schwerpunkt/d/Datenschutz.html>
 - 11 <https://www.computerwoche.de/hardware/data-center-server/2351470/>
 - 12 <http://de.wikipedia.org/wiki/Bundesdatenschutzgesetz>
 - 13 <http://h41112.www4.hp.com/promo/obc/de/de/business-it-advice/protect-your-business/how-to-improve-security.html>
 - 14 <http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=4408>
 - 15 <https://www.computerwoche.de/fileserver/idgwpcw/files/1870.pdf>
 - 16 <https://www.computerwoche.de/fileserver/idgwpcw/files/1872.pdf>
 - 17 <https://www.computerwoche.de/fileserver/idgwpcw/files/1888.pdf>
-

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.