

Millionenschäden durch gezielte Cyberangriffe auf Großunternehmen

Kaspersky-Umfrage: Im Schnitt kostet großen Unternehmen eine zielgerichtete Attacke 1,8 Millionen Euro, KMUs zahlen durchschnittlich 70.000 Euro

Moskau/Ingolstadt, 25. Juli 2013

Gezielte Angriffe auf Firmen können enorme Schäden verursachen, die von Großunternehmen mit durchschnittlich 1,8 Millionen Euro beziffert werden. Kleine und mittlere Unternehmen (KMUs) kostet eine zielgerichtete Attacke im Schnitt 70.000 Euro. Das ist ein Ergebnis einer weltweiten Umfrage, die Kaspersky Lab zusammen mit B2B International in diesem Jahr durchgeführt hat [1].

Cyberkriminelle kennen viele Möglichkeiten, Angriffe durchzuführen und wirtschaftliche Schäden zu verursachen. Gezielte Angriffe [2] gegen Unternehmen gehören dabei zu den gefährlichsten. Denn sie richten nicht nur den größten Schaden an, sondern sind in der Regel auch professionell organisiert und von langer Hand vorbereitet. Um an lukrative vertrauliche Unternehmensdaten zu kommen, setzen Cyberkriminellen oft auch erhebliche finanzielle Mittel und enormen Sachverstand ein [3].

Der Schaden zielgerichteter Attacken ist beträchtlich und wird von den von Kaspersky Lab befragten Unternehmen mit mehr als 1.500 Mitarbeitern auf durchschnittlich 1,82 Millionen Euro beziffert. Davon sind fast 1,65 Millionen Euro unmittelbar auf den Angriff zurückzuführen, sei es für die Beseitigung des Datenlecks, die Einschaltung externer IT-Spezialisten und Anwälte; oder in Folge einer schadensbedingten Einschränkung der Geschäftstätigkeit. Die restlichen 170.000 Euro wenden Unternehmen für präventive Maßnahmen auf, um ähnliche Vorfälle zukünftig zu vermeiden. Dazu zählen Investitionen in die Software und Hardware oder die Schulung von Mitarbeitern.

Doch auch in kleinen und mittleren Unternehmen (bis zu 1.500 Mitarbeiter) verursachen gezielte Angriffe enorme Kosten. Hier ergab die Kaspersky-Umfrage, dass die durchschnittlichen Verluste pro Angriff bei rund 70.000 Euro liegen, verteilt auf 55.000 Euro an direkten Kosten und 15.000 Euro für Präventivmaßnahmen.

Auch andere Angriffsformen auf Unternehmen können sehr teuer werden

Gezielte Attacken sind zwar die Angriffe mit den höchsten Folgekosten, aber keineswegs die häufigsten, denen Unternehmen ausgesetzt sind. Weltweit gesehen lassen sich derzeit etwa 9 Prozent aller Cyberangriffe auf zielgerichtete Attacken zurückführen. In Deutschland registrieren Unternehmen etwa 5 Prozent aller Angriffe als zielgerichtete Angriffe.

Weitaus mehr Angriffe, nämlich 24 Prozent weltweit, beziehungsweise 25 Prozent in Deutschland, betreffen Hacks des Unternehmensnetzwerks [2]. Auch Hacking-Attacken können hohe Folgekosten ergeben: Die gesamte durchschnittliche Schadenshöhe beträgt hier 1,27 Millionen Euro für Großunternehmen, bei kleinen und mittleren Unternehmen sind es 55.000 Euro.

Zudem ergibt die Kaspersky-Umfrage, dass fast jedes fünfte Unternehmen (19 Prozent) unter vorsätzlichen Datenlecks zu leiden hat, etwa über den Versand von E-Mails mit vertraulichen Daten oder den Einsatz mobiler Geräte von Mitarbeitern. Hier liegen die Kosten für Großunternehmen bei 743.000 Euro, für andere bei 39.000 Euro.

Die meisten Attacken richten sich mit 39 Prozent jedoch gegen Schwachstellen in der Unternehmenssoftware. Sie verursachen bei Großunternehmen Schäden von gut einer halben Million Euro, während kleine und mittlere Unternehmen davon im Durchschnitt mit 46.000 Euro belastet werden.

Innovative Technologie kann schützen

Da gezielte Angriffe auf Unternehmen von Cyberkriminellen akribisch vorbereitet werden, reicht der Einsatz von herkömmlicher Antiviren-Software alleine zum Schutz nicht aus. Vielmehr sind hier weitergehende, proaktive Maßnahmen notwendig.

Führende Lösungen am Markt wie Kaspersky Endpoint Security for Business [4] können auch sehr spezifische, gezielte Attacken auf Schwachstellen in der Unternehmenssoftware erkennen und verhindern – auch Zero-Day-Exploits. Über ein Whitelisting-Verfahren werden im Zusammenspiel mit anderen proaktiven Schutzmaßnahmen mögliche Schwachstellen in der Unternehmenssoftware erkannt und in einer Datenbank hinterlegt. Kaspersky Endpoint Security for Business bietet mit seiner dynamischen Whitelisting-Technologie ein von unabhängigen Experten anerkanntes Verfahren, das einen permanenten und weitgehenden Schutz von Unternehmensrechnern gewährleistet.

^[1] Die Umfrage wurde von B2B International im Auftrag von Kaspersky Lab im Jahr 2013 durchgeführt. Dabei wurden mehr als 2.895 IT-Entscheider aus 24 Ländern befragt – u.a. 117 deutsche. Es wurden Unternehmen jeglicher Größe erfasst, in drei Klassen von 10 bis 99 Arbeitsplätzen, über 100 bis 1.500 Arbeitsplätzen und Unternehmen mit mehr als 1.500 Arbeitsplätzen. Die Studie ist eine Fortführung von zwei früheren B2B International-Umfragen, die Kaspersky Lab mit ähnlichen Themen bereits im Jahr 2011 und 2012 beauftragt hat. Weitere Informationen zur aktuellen Studie „Global Corporate IT Security Risks: 2013“ können unter http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf abgerufen werden.

^[2] Unterschied gezielter Attacken und Hacker-Attacken siehe http://en.wikipedia.org/wiki/Targeted_threat und http://en.wikipedia.org/wiki/Hacker_%28computer_security%29

^[3] siehe Kapitel "Zielgerichtete Attacken" unter <http://www.viruslist.com/de/analysis?pubid=200883817#9>

^[4] <http://www.kaspersky.com/de/business-security>

Nützliche Links:

- Passendes Bildmaterial: <http://newsroom.kaspersky.eu/de/medien/bildmaterial/>
- Mehr zur Kaspersky-Umfrage: http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf
- Pressemitteilung zum Thema „Kostspielige Sicherheitsvorfälle: Größere Unternehmen können pro Cyberangriff rund eine halbe Million Euro verlieren“:

<http://newsroom.kaspersky.eu/de/texte/detail/article/kostspielige-sicherheitsvorfaelle-groessere-unternehmen-koennen-pro-cyberangriff-rund-eine-halbe-mi>

Über Kaspersky Lab

Kaspersky Lab ist der weltweit größte, privat geführte Anbieter von Endpoint-Sicherheitslösungen. Das Unternehmen zählt zu den vier erfolgreichsten Herstellern von Sicherheitslösungen für Endpoint-Nutzer.* In seiner 15-jährigen Unternehmensgeschichte hat Kaspersky Lab zahlreiche Innovationen im Bereich IT-Sicherheit auf den Weg gebracht und bietet effektive digitale Sicherheitslösungen für Großunternehmen, KMU und Heimanwender. Kaspersky Lab, mit Holding in Großbritannien, ist derzeit in rund 200 Ländern auf der ganzen Welt vertreten und schützt über 300 Millionen Nutzer weltweit.

Weitere Informationen zu Kaspersky Lab finden Sie unter <http://www.kaspersky.com/de/>. Kurzinformationen erhalten Sie zudem über www.twitter.com/Kaspersky_DACH und www.facebook.com/Kaspersky.Lab.DACH. Aktuelles zu Viren, Spyware, Spam sowie Informationen zu weiteren IT-Sicherheitsproblemen und -Trends sind unter www.viruslist.de und auf dem Kaspersky-Blog auf <http://blog.kaspersky.de/> abrufbar.

* Quelle: IDC-Report "Worldwide Endpoint Security 2012-2016 Forecast and 2011 Vendor Shares", July 2012.

Redaktionskontakt:

essential media GmbH
Florian Schafroth
florian.schafroth@essentialmedia.de
Tel.: +49-89-7472-62-43
Fax: +49-89-7472-62-17
Landwehrstraße 61
80336 München

Kaspersky Labs GmbH
Stefan Rojacher
stefan.rojacher@kaspersky.com
Tel.: +49-841-98-189-325
Fax: +49-841-98-189-100
Despag-Straße 3
85055 Ingolstadt

© 2013 Kaspersky Lab. The information contained herein is subject to change without notice. The only warranties for Kaspersky Lab products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Kaspersky Lab shall not be liable for technical or editorial errors or omissions contained herein.