Im Visier
Auch Google wurde bereits zum Ziel von Angriffen: Im Jahr 2009 durch chinesische Hacker.

Raubgut: Daten

Cyberangriffe nehmen immer mehr zu: Nutzerdaten von Millionen Kunden sind in Gefahr

LUXEMBURG
SVEN WOHL

Cyberattacken auf Großunternehmen sind längst keine Seltenheit mehr. Dabei handelt es sich nicht um ein Phänomen, das erst seit ein paar Jahren existiert, sondern das bereits seit längerem von sich reden macht. Da Unternehmen nur ungern Sicherheitslücken zugeben, dauert es oftmals lange, bis Informationen an die Öffentlichkeit gelangen. Wenn überhaupt.

Einer der aufsehenerregendsten Vorfälle der Vergangenheit stellt die Cyberattacke gegen Sony dar. Für mehrere Wochen musste im April und Mai 2011 der Online Dienst „PlayStation Network“ vom Netz genommen werden. Hacker hatten ihren Weg in die Datenbanken Sonys gefunden und über diesen Weg 77 Millionen Daten von Nutzerkonten entwendet. Über mehrere Tage hinweg wollte man bei Sony nicht zugeben, dass ein solches Problem tatsächlich existiere. Bei der amerikanischen Bank JP-Morgan dauerte es im vergangenen Jahr sogar Monate: Bekannt gemacht wurde der Angriff, bei dem 83 Millionen Konten frei gelegt wurden, im September, obwohl er im Juli stattfand. Komplett aufgehalten konnte der Angriff erst im Verlauf des Augusts.

Klar ist, dass diese beiden Beispiele nur die Spitze des Eisberges darstellen. International nehmen die Cyberangriffe auf Unternehmen jeder Größe zu. Wir haben Experten und Betroffene zu dieser Entwicklung befragt. ●

Nachholbedarf besteht

Beim „Chaos Computer Club Lëtzebuerg“ sieht man die Lage kritisch

LUXEMBURG Reine Profitgier steckt hinter dem Handeln von Hackern, die Cyberattacken ausführen. Jan Guth vom „Chaos Computer Club Lëtzebuerg“ (C3L) präzisiert, dass diese Hacker, die sich vom Ethik-Code losgesagt haben (mehr dazu im Infokasten), eigentlich Cracker genannt werden, um sie von den anderen Gruppen zu trennen. Er rät, dass sich jedes Unternehmen selbst up to date halten und jemanden einstellen sollte, der nicht nur von Informatik, sondern auch von Datenschutz Ahnung hat. Alternativ kann man sich auch an eine Firma, die sich darin spezialisiert hat, wenden.

Schwere Entscheidung
Im Falle eines Angriffes muss dann relativ schnell gehandelt werden.

Foto: Pierre Matgé

„Da muss der Verantwortliche für die Sicherheit immer abwägen, was er macht“, meint Jan Guth und präzisiert, dass beim Auftreten vieler Sicherheitslücken meistens nicht sofort eine Software-Lösung bereit steht. Die Wahl sieht wie folgt aus: Entweder die Online-Dienstleistungen, die man den Kunden anbietet, zurückfahren, um Angriffe zu vermeiden, oder riskieren, dass bei einer Attacke Kundendaten an Dritte gelangen.

Vor allem bei großen Unternehmen hat Jan Guth in dieser Hinsicht wenig Zuversicht. „Die haben das noch gar nicht im Griff. Da wird eher zuerst nach den Aktien geschaut“, erklärt er. Als Beispiel dient der Hackangriff auf Sony, wo erst reagiert wurde, als Anonymous diesen veröffentlichte. Erst dann wurde der Service für Wochen offline genommen. Kleine und Mittelständiges Unternehmen würden da schon besser handeln, denn wenn deren Ruf geschädigt sei, könne das ihre Existenz gefährden.

Der C3L wurde bereits mehrmals von Privatunternehmen kontaktiert. Meistens verweisen sie dabei auf den CIRCL und geben, falls das gefragt ist, zusätzlich eigene Ratschläge. „Da haben wir viel positive, aber auch einige negative Erfahrungen gemacht“, meint dazu Jan Guth.

SVEN WOHL

Mehr Informationen finden Sie auf www.c3l.lu

„Der Verantwortliche für die Sicherheit muss immer abwägen, was er macht“

JAN GUTH | Chaos Computer Club Lëtzebuerg

DEFINITIONEN

Drei Arten von Hackern

Hacker ist nicht gleich Hacker. Man unterscheidet zwischen drei verschiedenen Kategorien:

BLACK HAT HACKER, auch Cracker genannt, führen zur persönlichen Bereicherung Cyberattacken aus und schaden damit Unternehmen und Kunden.

WHITE HAT HACKER machen Sicherheitslücken in Systemen ausfindig und melden diese den Administratoren.

GREY HAT HACKER finden Sicherheitslücken, doch machen auf andere Art auf das Problem aufmerksam, falls die Betreiber sie ignorieren.

Mehr Informationen finden Sie auf: www.securitymadein.lu und www.circl.lu

Wiederholungstäter
Yahoo! wurde mehrmals angegriffen: Sowohl 2012 als auch 2013 und 2014 erhielten Hacker Zugriff auf die Datenbank.

Die Feuerwehr

„Security Made in Luxembourg“ hilft Unternehmen bei Cyberattacken

LUXEMBURG Bei Security Made in Luxembourg (SMILE) verfolgt man unter anderem das Ziel, der Privatwirtschaft und den Gemeinden im Falle einer Cyberattacke zu helfen. „Wir funktionieren ähnlich wie eine Feuerwehr“, erklärte uns Pascal Steichen im Interview. SMILE leisten bei einem solchen Vorfall erste Hilfe. Im vergangenen Jahr war das fast 3.000 Mal der Fall. Tendenz Steigend.

Internationale Steigerung

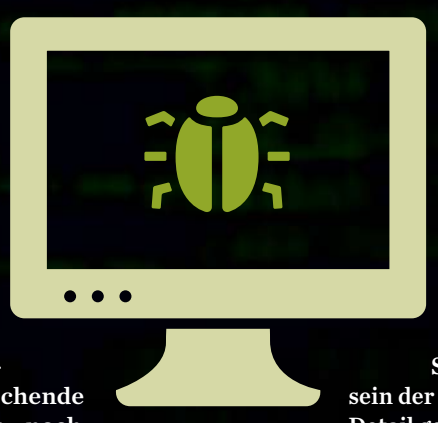
Das bedeutet natürlich nicht unbedingt, dass die Attacken in Luxemburg disproportional steigen oder Luxemburg immer attraktiver wird. Die Steigerung ist nämlich auf der ganzen Welt zu beobachten. Vor allem die organisierte Kriminalität nimmt zu, da sie immer mehr Interesse am Internet entwickelt.

Etwa die Hälfte der Fälle in Luxemburg entfallen auf den ICT-Sektor. Oft kommen die Meldungen zu den Fällen aus dem Ausland, die Betroffenen sitzen allerdings in Luxemburg. Doch die Situation verbessert sich: In den Unternehmen geht man immer reifer mit dem Thema um. Allerdings gibt es immer noch ein Problem bei der Aufspürung der Fälle: Bis solche Angriffe entdeckt werden, vergeht zu viel Zeit. Auch deshalb konzentriert man sich bei SMILE auch auf die Prävention, die sich sowohl an die Mitarbeiter als auch die Leiter eines Unternehmens richtet.

SVEN WOHL

Reale Gefahr

Wettlauf zwischen Unternehmen und Kriminellen



LUXEMBURG Wenn es um Hacking oder Internetbetrug geht, hat laut Justizsprecher Henri Eippers die Staatsanwaltschaft in Luxemburg noch eine sehr überschaubare Menge an Fällen zu bearbeiten. Maximal fünf im Jahr. Warum nicht mehr? Der Schaden ist für die Firmen zu gering – falls überhaupt einer entstanden ist, denn vielfach bleibt es bei abgewehrten Angriffsversuchen. Die IT-Abteilungen der Unternehmen oder die entsprechende Virensoftware ist schneller oder schlauer – noch.

Letzter bekannter Hackerfall In Luxemburg war, als ein Täter 2012 die Webseite von ArcelorMittal lahmlegte, wie der Unternehmenssprecher Pascal Moisy bestätigt: Der ermittelte belgische Anonymous-Aktivist habe damit gegen die Schließung der Anlage in Lüttich „protestieren“ wollen.

„Wir haben die Webseite aber schnell wieder online stellen können“, so Moisy. Der Fall zeigt aber, dass es in bestimmten Wirtschaftsbranchen wie dem Onlinehandel, ein gewisses Erpressungspotenzial darin steckt, wenn der Zugriff auf Webseiten blockiert wird.

Da anspruchsvollere Hackingangriffe aber auch anspruchsvolle Spezialisten verlangt, kommt es laut Eippers viel häufiger zu Ermittlungen gegen die Versender von eher primitiven Betrugs-Emails, in denen Mitarbeiter von Firmen beispielsweise an angebliche Anwaltskanzleien vermeintliche Rechnungen zu zahlen aufgefordert werden.

Wie Jean-Pierre Borsa, Senior Advisor und zuständig für Banking Technologies and Payments der Luxembourg Bankers' Association (ABBL) erklärt, sind zwar Banken von Hackingattacken bedroht, er sieht aber vielmehr noch die Gefahr bei den Bankkunden. Denn während sich die Banken der Gefahr bewusst seien und dagegen mit teurer Software schützten, wäre das Sicherheitsbewusstsein der Kunden nicht so ausgeprägt. Borsa möchte nicht ins Detail gehen, denn Diskretion gehört ja vor allem im Finanzwesen zum Geschäft, erst recht, wenn es um etwaige Schwachstellen geht. Dass die Gefahr da ist und auch angesichts zunehmenden E-Bankings nicht abnehmen wird, liegt für Borsa auf der Hand. Für Banken, so der IT-Sicherheitsfachmann des Bankenverbands, sei es darum überaus wichtig, dass E-Banking sicher bleibe, weshalb die Institute auch viel in die IT-Sicherheit investierten und die Kunden darüber informierten, wie sie sich gegen Angriffe schützen und Manipulationsversuche durch Phishing-Emails oder Trojaner vorbeugen und erkennen könnten. Borsa erklärt, dass es ausgesprochen schwer sei, IT-Systeme von Banken zu knacken. „Einfacher ist es da, Kunden mit falschen Links in den Emails auf gefährliche Seiten zu locken“.

MARCO MENG

Foto: Shutterstock

La Cybersécurité, c'est son affaire

Sogeti constate un boom des tentatives d'attaques au Luxembourg

BERTRANGE Au Luxembourg, Sogeti constate une hausse de 40% de la demande des entreprises par rapport au printemps de 2014 et même de 140% pour les tentatives d'attaques. À Bertrange, environ 30 des 550 salariés travaillent au sein des équipes Cybersecurity, incluant la participation au sein d'un laboratoire chargé de détecter des failles sur des produits software et hardware (laboratoire européen). Et pour mieux cerner la matière, «on utilise les mêmes armes et les mêmes modes de fonctionnement que les hackers», explique le Head of Security Business Development Vincent Laurens. La menace concerne tant les grandes que les petites structures, tous secteurs confondus. «Les sociétés prennent conscience de la valeur marchande de leurs données», ajoute le responsable. Qui plus est, une attaque impacte l'image des firmes et peut même pousser certains dirigeants à quitter leur poste.

Les «Advanced Persistent Threats»: discrets mais présents

La demande des entreprises varie selon leurs secteurs d'activités: la protection des données nominatives des clients et la sécurisation des flux transactionnels pour la finance, la sécurité des systèmes et les objets connectés pour l'industrie, tandis que dans les soins de santé, la protection du dossier médical des patients est sollicitée. Au Grand-Duché, Vincent Laurens constate une recrudescence des APT ou «Advanced Persistent Threats». Ces logiciels malveillants dorment dans les systèmes et déclenchent la capture de l'information à un moment bien précis. «Parfois, on compte douze ou 18 mois avant l'attaque», précise Vincent Laurens. La menace peut aussi se nicher dans les murs de l'entreprise, avec la complicité d'un hacker ou bien par la simple copie de données mais aussi involontairement, quand un salarié travaille sur un dossier confidentiel depuis son domicile, où l'ordinateur infecté collecte les informations. La menace est donc plus que jamais présente d'autant que les attaques sont de plus en plus ciblées. «Il y a un véritable changement d'environnement dans la cybersécurité», souligne le responsable de Sogeti.

CK

www.sogeti.lu