FOKUS: SECURITY

Die Krise als Übung

Ist Ihr Unternehmen gegen einen Cyber-Angriff wirklich gewappnet? Wie reagieren Mitarbeiter und Management, wenn Hacker einmal richtig zuschlagen sollten? Antworten auf solche Fragen liefern Krisenübungen, sogenannte War Games. → VON JENS STARK

Und plötzlich ist die Krise bittere Realität. Trotz vielfältiger Schutzmassnahmen und Mitarbeitertrainings ist die Firma Opfer eines massiven Hacker-Angriffs geworden. Heikle Kundendaten sind abhandengekommen, zudem wurden finanzielle Informationen abgeändert und verfälscht – und das bereits seit Wochen oder Monaten! Was nun?

In solchen Situationen stehen die meisten Unternehmen schlichtweg auf dem Schlauch. Die Leute, welche die Krise bewältigen sollen, sind komplett überfordert. Aus der Krise wird so leicht eine Katastrophe mit Folgekosten in Millionenhöhe, die das Überleben der Firma gefährden. «Viele Konkurse hätten in der Schweiz schon verhindert werden können, wenn die Unternehmen ein wenig in ihre Sicherheit und in ein professionelles Krisenmanagement investiert hätten», behauptet Richard Werner, Geschäftsführer von Risk Control RCC.

Der Mann kennt sich auf dem Gebiet aus: Seine Firma führt Krisenübungen für Kunden durch. In solchen auch War Games genannten Drills werden mögliche Krisenszenarien simuliert, um Unternehmensleitung und Mitarbeiter auf die Probe zu stellen.

Jens Stark
ist Redaktor der Computerworld mit den Schwerpunkten Networking und IT-Security

EIN DREHBUCH HÄLT ALLES FEST

Ein Cyber War Game läuft in mehreren Phasen ab. Es müsse sehr gut vorbereitet werden, sonst könne aus dem Spiel schnell bitterböser Ernst werden, warnt Werner. «Deshalb besprechen wir mit dem Kunden im Vorfeld die möglichen Worst-Case-Szenarien», erklärt er. Danach müssten bereits gewisse organisatorische Massnahmen getroffen werden, damit die Übung nicht ausser Kontrolle gerät.

«Bevor wir eine Übung abhalten, schreiben wir ein regelrechtes Drehbuch», so Werner weiter. Für die Übungen arbeitet Werner mit zahlreichen Freelancern zusammen, die zum Teil einschlägige Erfahrungen aus Geheimdiensten mitbringen. So kann er zum Beispiel Ex-Spione beiziehen, die einst dem britischen Auslandsgeheimdienst MI6 (Military Intelligence, Section 6), dem deutschen Bundesnachrichtendienst (BND) oder dem berüchtigten Ministerium für Staatssicherheit (Stasi) der ehemaligen DDR dienten. Natürlich informiere man die Firmen über den Hintergrund dieser Personen und arbeite mit diesen auch nicht zusammen, wenn die Auftraggeber dies nicht wünschten.

«Das fertige Drehbuch zeigen wir dem Unternehmen nicht», erklärt Werner. «Wir sagen der Firma nur, wir würden gern eine Krisenstabsübung mit einem IT-Szenario durchführen und holen uns die Erlaubnis des Top-Managements ein.» Das genaue Datum der Übung werde natürlich nicht genannt.

WICHTIGE CHECKLISTEN

Am Tag X wird der Krisenstab alarmiert, der aus vier bis sechs Leuten besteht. Dieser analysiert die Situation und fasst erste Entschlüsse. Das Wichtigste während der Krise seien Checklisten respektive ein zuvor ausgearbeiteter Krisenplan, meint Werner. «Ich habe schon Krisenmanager erlebt, die in einer Notsituation völlig überfordert waren, zusammengebrochen sind und dann von mir nach Hause geschickt werden mussten», berichtet er. An einem Plan kann man sich in solchen Fällen festhalten. Bei der Ausarbeitung eines Plans gibt es gewisse Rahmenwerke, die Checklisten selbst muss aber der Berater zusammen mit den Firmenvertretern im Team erarbeiten. Keinesfalls dürfe der Plan als 22-seitiger Prosatext daherkommen, er müsse aus wenigen Stichwortpunkten mit klarer Priorisierung bestehen, so Werner. «Zeit ist Geld und entscheidet über Erfolg oder Misserfolg!»

Nach der Übung verfasst Werner einen vertraulichen Bericht, in dem Stärken und Schwä-

CYBER WAR GAMES: DREI VORLAGEN

Viele Firmen, die bei Richard Werner und seiner Beratungsfirma Risk Control RCC anklopfen, sind gebrannte Kinder. Als Opfer von Attacken wollen sie nun besser gewappnet sein. Die Szenarien, die Werner und sein Ad-hoc-Team durchführen, sind zwar erfunden, sie basieren aber auf echten Vorfällen. Drei Beispiele:

1 Bei einer Bank wird Malware eingeschleust, die aber erst aktiv wird, nachdem alle Backups durchgeführt worden sind. Nach zwei Wochen wird in einem wichtigen Handelssystem bei den Beträgen die vierte Kommastelle verändert. Niemandem fällt etwas auf. Wieder werden alle Backup-Zyklen abgewartet, bis erneut Zahlen verändert werden. Irgendwann merken nicht nur die Firmenverantwortlichen, dass etwas nicht stimmt, sondern auch die Handelspartner. Grösste Herausforderung bei diesem Szenario: Niemand weiss, wann die Malware eingeschleust wurde und ob überhaupt noch «saubere» Backups zur Verfügung stehen.

2 Verärgerte IT-Mitarbeiter setzen den Serverraum unter Wasser. Einfach neue Server zu kaufen und die Daten vom Backup zu ziehen, stellt sich aber als schwieriger heraus als gedacht, denn das Überspielen der Daten aus einer zentralen Oracle-Datenbank dauert Tage statt Stunden. Fazit der Übung: Die Firma ist eine Woche ausser Gefecht gesetzt statt nur einen Tag. Der finanzielle Schaden in Form von Umsatzeinbussen geht in die Millionen. Die Versicherung zahlt aber nur 30 000 Franken.

3 Mitarbeiter einer Krankenversicherung sind laut Policy verpflichtet, nicht mehr benötigte Krankenakten und sonstige Dokumente von Versicherten zu schreddern. Im Szenario entsorgen sie die Dokumente jedoch offen im Container. Ein Mitarbeiter der Putzkolonne entdeckt die Papiere und informiert die Presse, um sich den «Leserreporter»-Lohn zu sichern. Die Folgen für das Unternehmen sind verheerend: Der Versicherung werden Verträge im Minutentakt gekündigt.

chen der Krisenbewältigung aufgezeigt werden. «Wir erstellen eine klassische SWOT-Analyse, in der wir etwa benennen, in welchen Bereichen die Krise gemeistert wurde, wo Handlungsbedarf besteht und wo das Unternehmen komplett durchgefallen ist», so der Berater.

Ein häufiger Schwachpunkt sei der Umgang mit den Medien. Hier sei nicht nur wichtig, was man berichte und wie, sondern auch wann. «Es nützt nichts, wenn man eine Pressemitteilung kurz nach Redaktionsschluss verbreitet, denn dann berichten die Medien bereits das, was sie wissen. Diese Informationen nachträglich zu korrigieren, ist sehr schwierig», führt Werner aus. Ohnehin ist im Krisenfall die Kommunikation das A und O, auch mit Behörden, Kunden und Mitarbeitern.

DISKUSSION UND WIEDERHOLUNG

Der Bericht ist zwar sehr ausführlich und beschreibt alle Phasen der Übung; wichtiger sei aber dessen Präsentation, die im Normalfall gut 45 Minuten dauert, betont Werner. «Bei dieser Gelegenheit kommen Fragen auf oder es werden andere Meinungen und Beurteilungen der Auftraggeber laut.» Dieser Prozess mündet in einem überarbeiteten und angepassten Dokument. «Hier wird über Massnahmen diskutiert, die anstehen», sagt er und gibt zu bedenken, dass ohne diese Art von Austausch der Bericht einfach in der nächsten Schublade verschwinden würde, ohne Wirkung bleibe und die ganze Übung im Grunde vergebens gewesen sei.

«Ich habe schon Krisenmanager erlebt, die in einer Notsituation völlig überfordert waren und zusammengebrochen sind»

Richard Werner, Risk Control RCC

Damit die Erfahrungen nicht wieder einfach vergessen gehen, müssten sie wiederholt werden, so Werner, am besten jährlich. «Wenn ein Unternehmen eine solche Übung nur einmal durchführt und dann fünf Jahre nicht mehr, muss die Firma ein neues Krisensystem aufbauen», gibt der Berater zu bedenken. «Meist sind dann die Leute weg, die dort bei der ersten Übung gearbeitet haben, und die neuen wissen gar nicht, was die Anforderungen sind», so der Fachmann weiter.

IN DER SCHWEIZ WENIG BEKANNT

Professionelle Krisenübungen sind in der Schweiz offensichtlich noch Mangelware. Werner schätzt, dass sie lediglich 8 bis 10 Prozent der Schweizer Unternehmen regelmässig durchexerzieren – vor allem grosse Unternehmen in der Finanzbranche und der Pharmaindustrie. Viele KMU weisen laut dem Experten aber ein «ganz grosses Manko» auf. Einzige löbliche Ausnahme seien Familienunternehmen. «Diese Patrons wissen, was sie zu verlieren haben, wenn ihnen das Unternehmen um die Ohren fliegt», führt er aus.

Laut Werner ist man in unserem nördlichen Nachbarland besser auf Ernstfälle vorbereitet. «20 bis 25 Prozent der deutschen Unternehmen setzen sich sehr stark mit dem Thema Krisenmanagement auseinander. Sie investieren dafür einen viel grösseren Teil ihres Budgets, denn sie haben erkannt, dass sie ganz anderen Bedrohungen ausgesetzt sind», beurteilt er die Lage. ←