www.sicherheit.info

PROTECTOR & WIK

Ausgabe März

SICHERHEITSTECHNIK & WIRTSCHAFTSSCHUTZ

3 / 2018

Titelthema

DIGITALISIERUNG IN DER SICHERHEITSTECHNIK

Top-Interview:
Stephan von Gündell-Krohne ist Beauftragter für Cyberthemen der Wirtschaft

IT-Sicherheit: Sicherheitslücken im IoT, Datenschutzgrundverordnung, Datenverwaltung in der Cloud, Jahresrückblick 2017

Zutrittskontrolle: Biometrie im Stadion, Identitäten im Smart Building, Normen in Großbritannien

Videoüberwachung: Einsatzgebiete für Wärmebildtechnik

ASW Bundesverband

Organ: ASW Bundesverband – Allianz für Sicherheit in der Wirtschaft e.V.

schlütersche

Betriebsspionage

Vor unsichtbaren Feinden schützen

Christian Schaaf

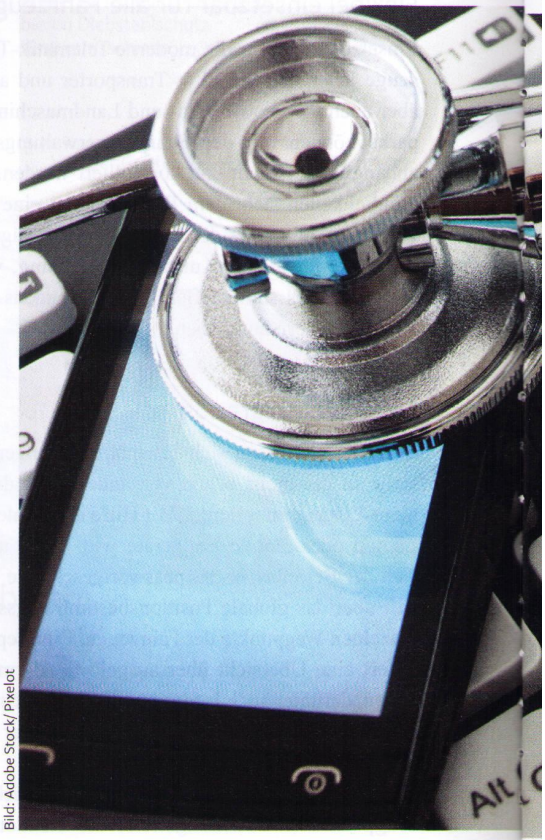


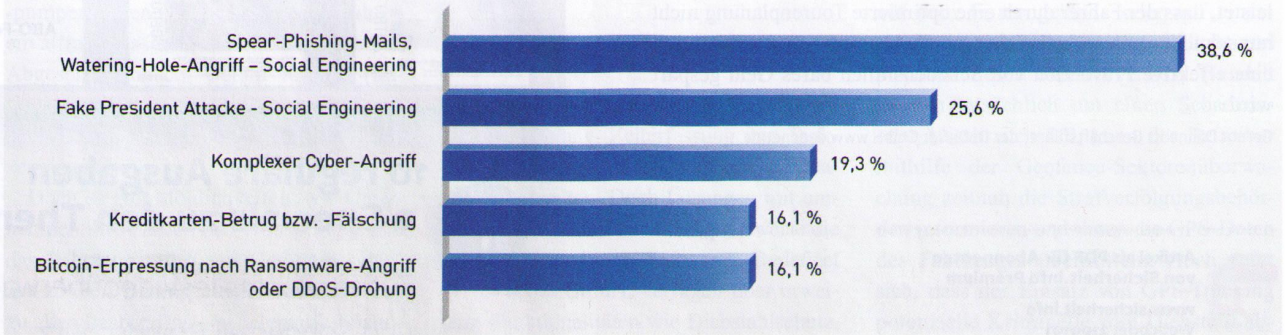
Bild: Adobe Stock/ Pixelot

Durch Betriebsspionage entsteht deutschen Unternehmen jedes Jahr ein Schaden in Milliardenhöhe. Der Faktor Mensch ist dabei oftmals die größte Sicherheitslücke, und die Angreifer gehen immer trickreicher vor, um ihre Opfer zu überlisten. Weil immer mehr persönliche Daten im Internet abgreifbar sind, können Kriminelle ihre Angriffe immer zielgerichteter vorbereiten. Gezielte – auf die Mitarbeiter ausgerichtete – Präventions- und Sensibilisierungsmaßnahmen helfen Unternehmen, sich vor den Tricks der Spione zu wappnen.

Etwa 30 Prozent aller befragten Unternehmen gaben in dem aktuell von Corporate Trust gemeinsam mit dem Bayerischen Verband für Sicherheit in der Wirtschaft (BVSW) und der Brainloop AG herausgegebenen Future Report an, Opfer von Spionage oder Informationsabfluss geworden zu sein. Über die Hälfte aller Unternehmen wurde in den letzten zwei Jahren bereits Opfer eines Angriffs durch die Organisierte Kriminalität, zum Beispiel durch Spear-Phishing-Mails oder eine Fake President Attacke (auch bekannt als CEO-Fraud). Befragt wurden für den Future Report, in dem die aktuellen Sicherheitsherausforderungen für Deutschland anhand der weltweiten Megatrends betrachtet wurden, 4.738 Vorstände, Geschäftsführer beziehungsweise Leiter der Bereiche Compliance, Risikomanagement, Unternehmenssicherheit, Informationsschutz, Recht, Finanzen, Controlling, Interne Revision, IT oder Personal.

Ahnungslos

Der Report zeigt deutlich die Gefährdungslage der deutschen Wirtschaft, nicht zuletzt aufgrund der Ahnungslosigkeit vieler Unternehmen. So konnte ein Viertel aller Unternehmen (exakt 25,6 Prozent), abgesehen von den konkreten und belegbaren Fällen, gar nicht sagen, ob sie bereits angegriffen wurden oder nicht. Hier fehlen vermutlich entsprechende Systeme und Prozesse, um einen solchen Angriff überhaupt feststellen zu können – leider symptomatisch für viele Firmen. Vielen Menschen fällt die realistische Beurteilung der Gefahrenlage schwer, und im Zweifelsfall sind die anderen immer mehr bedroht als man selbst. Auf die Frage, welche Gefahren sie durch Industrie 4.0 beziehungsweise IoT für die deutsche Wirtschaft allgemein und konkret für ihr eigenes Unternehmen sehen, gaben 83,9 Prozent an, dass sie Cyberattacken in Zukunft für die größte Bedrohung für die deutsche Wirtschaft halten. Konkret für ihr eigenes Unternehmen schätzen dies jedoch nur 66,5 Prozent als Bedrohung ein. Die zunehmende Abhängigkeit vom Internet sehen zwar 80,7 Prozent als Gefahr für die deutsche Wirtschaft, jedoch nur in 51,6 Prozent auch als Gefahr für ihre eigene Firma.



Grafik: Corporate Trust 2017

Welche Schäden erlitten Sie durch einen solchen Angriff durch die Organisierte Kriminalität? (Mehrfachnennungen möglich).

Die Angreifer suchen gezielt nach Informationen über die Mitarbeiter – im gehackten Firmennetzwerk, im Darknet oder in den Sozialen Medien.

Der User im Zentrum der Prävention

Die Bedrohung durch Betriebsspionage wird trotz hoher Schäden also immer noch häufig unterschätzt. Weder Manager noch Mitarbeiter rechnen mit Spionageangriffen, obwohl sie quer durch alle Branchen an der Tagesordnung sind und für viele Geheimdienste zum Tagesgeschäft zählen. Die präventiven Maßnahmen müssen sich nicht nur auf die stärkere Absicherung der IT- und Telekommunikationssysteme stützen, sondern vermehrt um die User kümmern. Denn sie werden in Zukunft noch viel häufiger die Angriffsziele sein. Bei der Prävention in den Unternehmen sollte dabei allerdings mehr Wert auf Sensibilisierung und Unterstützung der Mitarbeiter beim Verstehen der digitalen Prozesse gelegt werden als auf Kontroll- und allumfassende Überwachungsmaßnahmen.

Denn längst sind moderne IT-Systeme und Firewalls so gut, dass sie Spionageattacken zum Beispiel über Schadsoftware oder über an Mitarbeiter geschickte Werbe-E-Mails mit Trojaner-Anhängen rechtzeitig erkennen und in der Regel verhindern können. Außerdem sind die meisten Mitarbeiter inzwischen sensibilisiert, nicht mehr bedenkenlos auf jeden schlecht gemachten E-Mail-Anhang zu klicken.

Hier jedoch wurzeln die aktuellen Herausforderungen. Denn Täter gehen heute sehr viel gezielter vor. Während früher mit einem E-Mail-Massenversand möglichst viele Rechner beziehungsweise Unternehmen angegriffen wurden („Gießkannenprinzip"), um den Schadcode durch unachtsame User auf alle schlecht gesicherten Rechner zu bringen, sind die Angriffe heute ganz zielgerichtet. Während früher einfach möglichst viele Informationen und Daten erbeutet werden sollten, geht es den Tätern heute ganz konkret um einzelne Unternehmen oder bestimmte Technologien. Wenn eine Angriffsmethode (zum Beispiel Trojaner in E-Mail-Anhängen) nicht funktioniert hat, bedeutet dies noch lange nicht, dass sie aufgeben. Der moderne „Angriffsbaukasten" sowohl der Nachrichtendienste als auch der Industriespione und der Organisierten Kriminalität (OK) bietet eine Vielzahl von Möglichkeiten, um sich einen Zugang ins Firmennetzwerk oder auf bestimmte Computer zu verschaffen. Die Täter versuchen so viele Methoden und greifen so lange an, bis sie an ihr Ziel kommen. Man spricht in diesem Zusammenhang von langanhaltenden und nachhaltigen Angriffen, „APT"-Angriffen (Advanced Persistent Threat).

Täter nutzen ein Opfer als Einfallstor

Dazu spionieren die Täter ihre Opfer bis ins Persönlichste aus. Sie recherchieren oft über mehrere Wochen zunächst die genauen Ansprechpartner, um im Weiteren deren Hobbies, Freunde, frühere Arbeitgeber oder gebräuchlichen Redewendungen im Unternehmen auszuforschen. Sie nutzen dazu soziale Netzwerke oder im Darknet gekaufte Informationen über Zugangsdaten, die zuvor bei einem Hack auf ein Portal erbeutet wurden. In Zukunft werden dies auch viele Informationen sein, die über schlecht gesicherte Server von Wearable -Anbietern abgegriffen werden, denen wir bedenkenlos unsere Daten übermittelt haben. Mit diesem Wissen können die Täter ganz gezielte Angriffe erstellen, zum Beispiel sehr persönliche E-Mails, die von den Usern kaum mehr von Echt-E-Mails, die sie den ganzen Tag im Geschäftsbetrieb erhalten, unterschieden werden können.

Damit Unternehmen sich vor solchen Attacken schützen können, müssen die Mitarbeiter erst einmal überhaupt wissen und verstehen, wie die Täter heute vorgehen, wie kritisch es ist, sämtliche persönliche Daten in sozialen Netzwerken oder allen möglichen sonstigen Stellen im Internet einzugeben. Sie müssen sensibilisiert werden, wie leicht es ist, sie darüber auszuforschen und anschließend gezielt zu manipulieren. Für solche Maßnahmen gibt es allerdings derzeit in den wenigsten Unternehmen eine geeignete Stelle. Theoretisch wäre die Personalabteilung fachlich zuständig für die Schulung von Mitarbeitern, doch fehlt ihr in der Regel das entsprechende Know-how. Die IT-Abteilung, bei der dieses Know-how vorhanden sein sollte, wird hingegen in den meisten Fällen nicht als zuständige Stelle für die Schulung der Mitarbeiter wahrgenommen.

Fachübergreifende Taskforce

Um die unternehmenseigenen Kronjuwelen in Zukunft effektiv(er) vor digitalen Spionageattacken zu schützen, ist es notwendig, die Präventionsmaßnahmen auf derartige Angriffe mit allen in diesen Bereich involvierten Abteilungen abzustimmen. Neben der IT und dem HR-Bereich muss auch die Compliance miteinbezogen werden, um sowohl Regularien für die Kontrolle der IT-Geräte aufzustellen, jedoch im Gegenzug auch auf das Augenmaß bei der Umsetzung solcher Kontrollen zu achten. Außerdem sollte sich auch die Geschäftsleitung intensiv mit dem Thema befassen. Erstens sind gerade die Top-Manager in nicht unerheblichem Maße das Ziel solcher Angriffe. Zweitens werden entsprechende Budgets sowohl für die Härtung der IT-Infrastruktur wie auch für die Sensibilisierung der Mitarbeiter erst dann freigegeben, wenn dem Management bewusst ist, wie wichtig solche Maßnahmen sind. Schließlich ist es gerade bei der Umsetzung von Sensibilisierungsmaßnahmen für Mitarbeiter wichtig, dass das Management mit Vorbildfunktion voran geht und alle – vom Mitarbeiter bis zum Manager – die Maßnahmen mittragen. Nur so werden sich Unternehmen zukünftig wirksam vor Betriebsspionage schützen können.

Christian Schaaf, Geschäftsführer der Corporate Trust, Business Risk & Crisis Management GmbH, www.corporate-trust.de