Dipl.-Ing. Günter Holzhauser, Sebastian Schramm

Digitaler „Finger- und Fußabdruck“ von Mensch und Organisation im Cyberraum

Eine rasant zunehmende Gefährdung

Die immer schneller voranschreitende Vernetzung und Digitalisierung unseres Lebens im Kontext von z.B. Internet der Dinge, Industrie 4.0, Social Media, Connected Mobility und Smart Home stellt nicht nur die Sonnenseite unserer digitalen Evolution dar. Günter Holzhauser hat bereits verschiedentlich im cpm forum zu Themen der IT-Sicherheit geschrieben und auf deren Bedeutung hingewiesen.

Wo viel Sonne ist, ist auch viel Schatten. Diese Schattenseiten stellen eine zunehmend hohe Gefährdung für Mensch und Organisation dar, da man sich mit dem digitalen „Finger- und Fußabdruck“ in der Regel nicht beschäftigt, den man gewollt oder ungewollt im Cyberraum hinterlässt. Diese fehlende Transparenz stellt ein Risiko dar, da der digitale „Finger- und Fußabdruck“ mit frei verfügbaren oder kommerziellen Methoden und Tools aufgeklärt und sichtbar gemacht werden kann. Selbst nur halbwegs versierte Kriminelle finden aus den Ergebnissen dieser Aufklärung eine Unmenge von Informationen, die für gezielte Angriffe auf Personen und Unternehmen geeignet sind. Sabotage von IT-Infrastruktur, Erpressung, Desinformationskampagnen, Informations- und Datendiebstahl sind dann die Folgen.

OSINT Open Source Intelligence – Methoden und Tools von Geheimdiensten entwickelt und von Kriminellen eingesetzt

Zu Beginn steht das Tactical Information Gathering, also die Informationsbeschaffung nach Zielvorgabe. Von der organisierten Kriminalität wird die passive Aufklärung mit den Methoden und Tools der OSINT Open Source Intelligence durchgeführt. Im Weltmarkt gibt es viel Applikationen und Softwareprogramme, die eigens für diese Zwecke entwickelt wurden. Es muss mit Erschrecken festgestellt werden, dass heute alles – aber auch alles – mit OSINT so aufgeklärt werden kann, um Dritten (Mensch oder Unternehmen) zu schaden.

Die Zusammenführung von Einzeldaten zur Information ist die Gefährdung

Die Beschaffung der öffentlich verfügbaren Informationen über eine Person dauert in der Regel nur wenige Tage. Klick für Klick füllte sich das Dossier der Angreifer. Namen und Adressen von Mitarbeitern, ihre E-Mail-Adressen, Telefonnummern, Sozialen Medienprofile, Chats, Hobbys, Namen von Schulkameraden und Familienmitgliedern, private Fotosammlungen, berufliche Vorträge, Arbeitgeber, Funktion und Konferenzteilnahmen und vieles mehr.

Anhand von Handelsregistern und Firmenverzeichnissen lassen sich selbst komplexe Firmenstrukturen entschlüsseln. Karriere-Netzwerke wie LinkedIn und XING geben nicht nur die Namen einzelner Mitarbeiter preis, anhand deren Profi-

METHODEN DER INFORMATIONS-BESCHAFFUNG

Kritische Sicherheitslücken!

Der Server ist anfällig für die POODLE Attacke	116
Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2) wird vom Server akzeptiert	113
Der gebrochene RC4 Algorithmus kann verwendet werden	106
Offener Port für das gesamte Internet sichtbar, der in der Vergangenheit von Hackern angegriffen wurde	4
Die Verschlüsselung kann abgeschaltet werden	2
Der Server ist anfällig für die ROBOT Attacke	1
Der Server ist anfällig für CCS Injection	6
Der Server ist anfällig für die Heartbleed Attacke	6
Der Server ist anfällig für die Angriffe auf die Renegotiation	5

Mitarbeiterverhalten im Internet

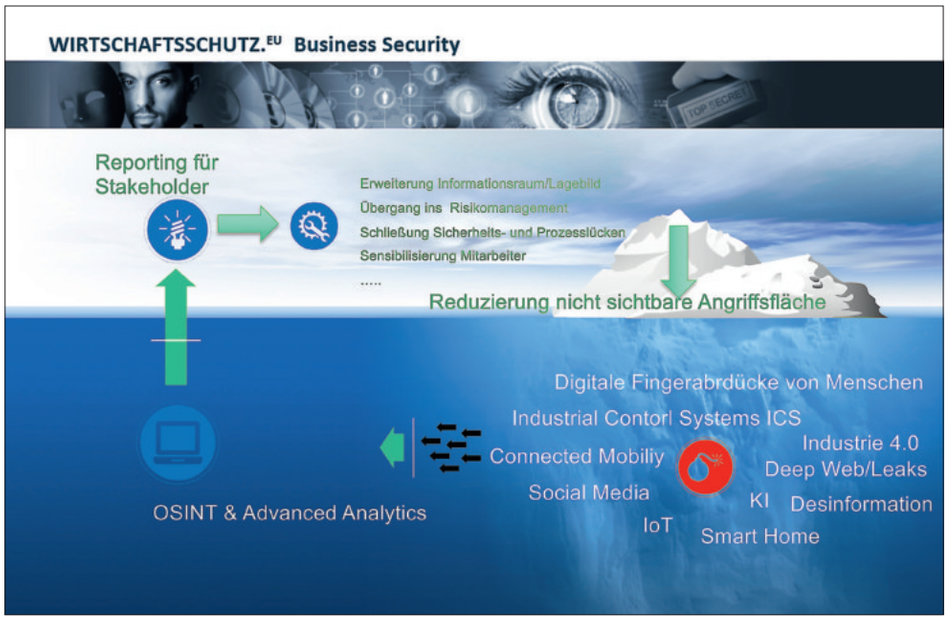
Die Verwendung von Firmen E-Mailadressen im Internet birgt vielfältige Gefahren. Insbesondere wenn Privates und Berufliches sich vermischen steigt die Gefahr eines ungewollten Informationsabflusses. Dazu kommt ein eventueller Reputationsschaden. Für die Domains in diesem Bericht wurden folgende problematische Verwendungen entdeckt:

	# verwendete Firmen E-Mailadressen
Soziale Netze & Chatplattformen	32
Video- & Musikportale	15
Filesharingdienste, P2P Netzwerke & Tauschbörsen	26
Spieleplattformen & Gamingforen	6
Hackerforen	0
Datingseiten	53
Erotik- und Pornoseiten	0

Alle Abb.: Autor

le lassen sich auch Rückschlüsse auf die Binnengliederung des Unternehmens sowie aktuelle Projekte, an denen sie arbeiten, ziehen. Über die Firmendomain und den Mitarbeiternamen lassen sich dann im Handumdrehen die personenbezogenen Firmen-E-Mail-Adressen – etwa nach dem Schema {Vorname}.{Nachname}@firmendomain.com – mit einfachen Tools im Internet generieren und verifizieren. Die Selbstdarstellung der Mitarbeiter in den Sozialen Netzwerken liefert zusätzliches Material über deren Privat- und Familienleben.

Nach und nach entstehen so detaillierte Profile, aus denen die Angreifer die vielversprechendsten auswählen können. Z.B. leitende Mitarbeiter oder deren persönliche Assistenten aus den Bereichen wie Vorstand, Forschung & Entwicklung, Konstruktion oder Vertrieb. Je mehr die Angreifer an Details zu einem Mitarbeiter sammeln konnten, umso höher die Wahrscheinlichkeit, dass sie diesen gezielt durch Social Engineering manipulieren können.



WER SEINEN DIGITALEN FINGER- UND FUSSABDRUCK KENNT, KANN GEGENMASSNAHMEN EINLEITEN

Die technische Aufklärung von Organisationen und Unternehmen ist eine massive Gefährdung

Ein enormes Risiko ist die Aufklärung der IT-Infrastruktur einer Organisation. Mit den geeigneten Methoden und Tools aus dem Werkzeugkasten der OSINT Open Source Intelligence lassen sich z.B. Informationen über Domain, Subdomain, IP-Adressen, die Verschlüsselung (Zertifikate, Algorithmen), IT-Provider, IT-Partner, Servereinstellungen/Ports, Zugänge für Fernwartung Blacklisting, Verhalten der Mitarbeiter im Cyberraum, gehackte Accounts und gehackte Passwörter (im Klartext) oder sogar Hashwerte ermitteln.

Auch über den Unternehmenssitz selbst lässt sich auf dem OSINT-Wege viel Nützliches herausfinden. Selbst gut geschützte Firmen in Industrieparks, die mit CCTV-Kameras, elektronischen Zugangssystemen und Wachschützern ein hohes Maß an Sicherheit bieten, lassen sich aufklären. Die Angreifer fanden zum Beispiel Grundrisse des Industrieparks mit allen Gebäudebeschriftungen und Firmenzuordnungen, Fotos und sogar Videos bei Youtube über die Sicherheitssysteme bis hin zu der genauen Leistungsbeschreibung der Sicherheitskameras, eine Illustration der Sicherheitsprozesse, die Besucher durchlaufen müssen, sowie eine Busrundfahrt um das Geländer herum, bei der auch die Höhe der Schutzzäune und Platzierung der Kameras sichtbar war. All diese Informationen sind für eine physische Infiltration der Firma verfügbar, ohne überhaupt vor Ort sein zu müssen.

Diese Daten in Summe ergeben ein erstes klares Lagebild über den Zustand der Sicherheit eines Unternehmens oder seine IT-Infrastruktur. In falsche Hände gelangt, lassen sich sofort Ansatzpunkte für einen gezielten und effektiven Angriff auf ein Unternehmen finden. Gerade der Bereich der Server und Verschlüsselung zeigt oft massive Sicherheitslücken, die von einem Angreifer sofort ausgenutzt werden könnten.

Ein hohes Risiko stellt auch das Nutzungsverhalten der Mitarbeiter eines Unternehmens dar. Mit Firmenaccounts sind nicht wenige Mitarbeiter (fast immer auch IT-Admins) auf fragwürdigen und riskanten Internet-Plattformen unterwegs. Anhand einer OSINT-Aufklärung lässt sich herausfinden, dass Mitarbeiter mit ihren Firmenpasswörten z.B. im Bereich Dating, Seitensprung, Pornographie, Darknet, Raubkopie (Musik und Filme) sowie Sozialen Netzwerken (Chat) unterwegs sind. Aus diesen Informationen lassen sich schnell Ansatzpunkte für den Angriff auf die Person oder das Unternehmen finden. Denn oft verwenden die Mitarbeiter bei diesen Aktivitäten die gleichen Passwörter, die sie auch an ihrem Arbeitsplatz verwenden. Das Nutzungsverhalten des Mitarbeiters im CyberRaum ergibt oft auch Erpressungspotenzial gegen die Person selbst.

In einem Fall war es sogar so, dass der Geschäftsführer des Rechenzentrums (verheiratet, mit zwei kleinen Kindern) auf verschiedenen Seitensprung- und Datingportalen aktiv war. Diese Gegebenheit wäre ein Bilderbuchfall für eine gezielte Erpressung des Geschäftsführers.

OSINT ist dabei mehr als nur eine Suche bei Google. Deep Web, Dark Web, Industrie 4.0, Internet of Things (IoT) – diese Schlagworte deuten auf die Bandbreite der Recherche-ansätze, die sich potentiellen Angreifern bieten. Im digitalen Zeitalter hat heute jeder Zugriff auf hochauflösende Satellitenbilder (Imagery Intelligence, IMINT), darauf hatten früher nur Nachrichtendienste Zugriff.

Wie lässt sich das Risiko reduzieren?

Transparenz und Kenntnis der eigenen Angriffsfläche im CyberRaum wird in unserer vernetzten und digitalen Welt zunehmend wichtiger. Nur wer seinen digitalen Finger- und Fußabdruck kennt, kann Maßnahmen zur Reduzierung der Angriffsfläche einleiten und das Risiko eines Angriffes reduzieren.

Funktionierende Prozesse der Sicherheit und geschulte Mitarbeiter sind ein wesentlicher Beitrag für das Bild im CyberRaum. Die neuen Themen der Digitalisierung und die Security müssen zukünftig Hand in Hand gehen. ■