Die moderne Form des Wissenszuwachses

Die Aufklärung

Forum für Informationssicherheit

ist die Grundlage jeder Spionage.

Denn sie können nur dort erfolgreich sein, wo das Wissen ist, das sie sich aneignen wollen. Damit beginnt Ihre erste Aufgabe um erfolgreich zu dem Wissen zugelangen, was sie erlangen möchten.

Die Anzahl dieser "Wissensquellen" ist im kybenetischen Raum gewaltig groß. Sie müssen jetzt nur noch selektieren, wo sich das von ihnen angestrebte Wissen befindet.
Auch hierzun gibt es eine ganze Reihe von Methoden, die aus der klassischen Spionage kommen. Es soll auf diese nicht eingegangen werden, Da sie die Spezifik des kybernetischen Raumes sprengen würde. Jedoch ist es sehr wichtig auf die Informationen aus diesem zurück greifen zu können.
Vielfach sind offene Quellen ein sehr interessanter Hinweis. Denn sie wissen ja, laut Putin kommen **100 % der Informationen oder des Wissens aus offene Quellen. Dieser Mann muß es ja wissen.**

Sie müssen jetzt nur noch dieses Wissen in den kybernetischen Raum transformieren. Was nicht anders heißt, sie müssen die Zielobjekte ihres Hungers nach Wissen, ermitteln. Der Vergleich mit der Stecknadel im Heuhaufen ist hier angebracht, jedoch ist das Verhältnis Heuhaufen zu einer Stecknadel wesentlich größer, denn sie haben es mit einem "globalen Netzwerk" zu tun.
Also viel Spass bei der Suche.

Aber, vielleicht ist diese Suche nicht doch so umfangreich ?

Versuchen sie es mal mit Hilfe der "Suchmaschinen" zu optimieren.

Das Ergebnis ist jetzt ein kleinerer Berg an möglichen Zieladressen. Die Betonung liegt auf der Formulierung "möglichen", sie wissen ja selbst, wie nachlässig man mit "Schlüsselwörtern" umgeht.

Bevor sie weitere Schritte unternehmen, müssen sie diese Zieladressen bewerten. Welche Erwartungshaltung haben sie, das die von ihnen gewählte Zieladresse auch das von ihnen gewünschte Wissen beinhaltet ?

Da haben es die "klassischen Nachrichtendienste" einfacher.

Jetzt haben sie einen überschaulichen Berg an Zieladressen, von dem sie glauben, er enthält ihr "fehlendes Wissen, das sie durch Spionage erweitern müssen..

Gegenmaßnahmen:
liquidieren sie alle Informationen mit einem Bezug auf sensible Informationen ihres Unternehmens im kybernetischen Raum (das sind alle Informationen, die ihnen den Mehrwert schaffen) auf den "Kraken", eine andere Bezeichnung für die "Suchmaschinen", für ein gut gemeintes System, dass sich in diesem Falle in das Gegenteil verkehrt.)
Es geht in diesem Falle nur um die Informationen, die sie selber in das globale Informationssystem gestellt haben.
Sie selber haben diese Information veröffentlicht !

Die Zielanalyse

Vor ihnen, dem möglichen Angreifer, liegt ein Berg an Zieladressen über mögliche Ziele.

Jetzt kommt die Phase der Zielbestimmung, denn man möchte ja nicht umsonst Spionagemittel verschwenden, auch wenn es einige tun. Welche Mittel dort eingesetzt werden hängt im Allgemeinen von einer ganzen Reihe von Faktoren ab, Dies können "klassische Verfahren" sein, genauso wie ein Angriff aus dem kybernetischen Raum, oder aber auch kombinierte Aktionen sind möglich. Dafür ist entscheident, welchen Wissenzuwachs man erwartet. Gleichzeitig spielt natürlich auch der Sicherheitsstandard eine Rolle, mit dem sie ihre Informationen (Wissen) schützen. Diese Phase ist die Zeit der Analytiker, sie müssen festlegen, welche Zieladressen vorrangig zu "untersuchen" sind und welche eine geringere Priorität haben.

In dieser Phase, sind sie als mögliches Zielobjekt zur Untätigkeit verdammt. Sie fühlen sich wie "das Kaninnchen vor der Schlange", Sie müssen abwarten, ob ihre Informationen "wertvoll" sind, im Sinne der Anforderungen des Auftraggebers, der einen Wissenzuwachs erzielen will.

In dieser Phase erfolgen keine Aktivitäten, aus denen erkannt werden kann, ob oder nicht, sie ein Angriffsziel sind.

Gegenmaßnahmen : keine
Sie fühlen sich wie "das Kaninchen vor der Schlange",

Die Methoden zum Eindringen in das Zielobjekt

Wenn die Entscheidung gefallen ist, in das Zielobjekt einzudringen, wissen immer noch nicht, ob sie dazu gehören oder nicht. Sie fühlen sich immer noch wie "das Kanninchen vor der Schlange". Aber lange halten sie diesen Zustand nicht aus, entweder brechen sie zusammen oder sie lernes es mit diesem Zustand zu leben.

Sie haben doch bereits lange mit disem Zustand gelebt, warum verfallen sie jetzt in diese Hektik ? Na gut, ihre Informationen sind Milliiarden US $ wert. Für den "richtigen Empfänger" lassen mit diesem, ihren Wissen, wesentlich mehr als die von ihnen genannten Milliarden verdienen.

Sollte der Wert ihrer Informationen und damit das zugehörige Wissen, auch bedeutend kleiner sein als die obengenannte Summe, es reicht auch, um sich wie vor einer Schlange zu fühlen.

Jetzt brauchen sie sich noch keine "Sorgen" machen.

Vor welchem Problem steht denn jetzt der "mögliche Spion" ?

Dies ist die entscheidenste Frage, wobei sie nicht eindeutig beantworten läßt, wählt er die "klassische Methode" oder die "kybernetische Methode" oder aber einen Mix aus beiden Varianten.

1. die klassische Methode
diese Methode wird dann gewäht, wenn bereits "menschlikche Quellen" im Zielobjekt vorhanden sind. Dabei kann die "klassische Form" der Informationsgewinnung angewendet werden..Als weitere Möglichkeit besteht durch einen direkten Angriff auf die kybernetische Einheit des Zielobjektes ohne Nutzung des kybernetischen Raumes durch die vorhandenen menschlichen Quellen. **(Angriffspunkte - der Mensch - bzw. die Input bzw Output Kanäle)**

2. die kybernetische Methode
wenn bereits detaillierte Informationen zur kybernetischen Einheit des Zielobjektes vorliegen, die einen zielgerichteten und erfolgreichen Angriff der Spionagemittel gewährleisten.
sollten diese Informationen nicht vorliegen, ist durch einen vorgeschalteten Angriff, das Zielobjekt aufzuklären.
Diese Angriffe erfolgen direkt aus dem kybernetischen Raum unter Nutzung der Ressourcen der kybernetischen Einheit. **(Angriffspunkt - die Online Kommunikation zum kybernetischen Raum)**

3. die Mix - Methode
Diese Methode stellt wie der Name bereits sagt einen Mix aus Klassik und Moderne dar.
Der Angriff erfolgt aus dem kybernetischen Raum (Cyberspace) mit oder ohne Ünterstützung der im Zielobjekt vorhandenen menschlichen Kapazitäten. Das "gewonnene Wissen" wird per kybernetischen Raum an den Auftraggeber gesendet.

Der Angriff erfolgt aus dem kybernetischen Raum (Cyberspace) mit oder ohne Ünterstützung der im Zielobjekt vorhandenen menschlichen Kapazitäten. Das "gewonnene Wissen" wird durch die menschlichen Quellen an den Auftraggeber gesendet.

Der Angriff erfolgt mit Ünterstützung der im Zielobjekt vorhandenen menschlichen Kapazitäten. Das "gewonnene Wissen" wird per kybernetischen Raum an den Auftraggeber gesendet.

Gegenmaßnahmen :
Haben sie alle erforderlichen Schutzmaßnahmen getroffen ?
Wenn nicht, dann könnte es jetzt schon zu spät sein !
Sind ihre Schutzmaßnahmen dem Wert der Information angepaßt ? Achten sie dringend auf die Angriffspunkte

Die Informationsbeschaffung

Dieses Ereignis werden sie leider nicht erleben, oder es sei, die "Einbrecher" sind stümperhaft vorgegangen.

Der Begriff "Einbrecher" wurde bewußt gewählt, denn sie wissen, es kann sich um klassische Einbrecher oder Mitarbeiter ihres Unternehmen handeln; es können aber auch "kybernetische Pfeile" mit ihrem hochintelligenten Spektrums um an ihre Informen zugelangen; oder aber auch um die Kombination beider Methoden handeln.
So kann es pazieren, das die "Einbrecher" mehrfach ihre "kybernetische Einheit heimsuchen. Nicht etwa, weil er was vergessen hat, nein, weil er beim ersten Einbruch noch nicht alles mitgenommen hat.
Zu diesem zweiten Einbruch nutzte er die gleichen Wege, wie beim ersten Mal, denn sie haben bis heute noch keine Ahnung, das ihre kybernetische Einheit einen oder mehrere Tage der "offenen Tür" hatte.
Um die "Einbrecher" auf frischer Tat zu erwischen, müssen sie Ihr Sicherheitsniveau so erhöhen, das den Anforderungen moderner Sicherheitsanforderungen entspricht. Ihre Schwachstellen kennen sie ja bereits, Sie wissen also, was sie dringend machen sollten. Analysieren sie den Wert ihrer Informationen - oder anders ausgedrückt - den Wissenzuwachs für den Auftraggeber der Einbrecher. Sollte es trotzdem zu zeitlich verzögerten Schädigungen ihres Unternehmens kommen und sie am Ende die Insolvenz anmelden müssten, dann haben sie an einer entscheiden Stelle "falsch gehandelt".
Sie haben nur an einer Stelle falsch gehandelt, sie haben ihren "Konkurrenten sträflich unterschätzt. Er macht jetzt ihren Gewinn !

Die zeitliche Einordnung der Informationsbeschaffung, sie erfolgt grundsätzlich nach derZielplanung und der Auslösung der Operation zur Informationsgewinnung.
Wann Sie beginnt, bestimmt der Angreifer, wann sie endet, wird von verschiedenen Faktoren bestimmt :
- die erforderlich Zeit um alle relevanten Informationen "auszukehren";
- bei der Analyse werden weitere wichtige Informationen entdeckt, die eine Erweiterung der Operation erforderlich machen;
- die Operation wird in zeitlichen Intervallen fortgeführt, da sich dies aus der Informationsanalyse ergibt;
- die Analyse de Sicherheitsmaßnahmen ergab keine Veränderungen zu den bereits vorliegenden Informationen;
- das Operationsobjekt verfügt nicht über die gewünschten Informationen; Fehloperation
- die interessante Informationsmenge wurde bereits umgekehrt, keine weiteren Informationen geringe Ergiebigkeit des Zielobjektes - Zielobjekt leer
- keine strukturierten Informationen gefunden; fehlerhafte Analyse des Zielobjektes
- Zugang zu den Datenbanken blockiert; fehlerhafte Analyse des Zielobjektes
- kein Zugriff auf die Informationen möglich; fehlerhafte Analyse des Zielobjektes

Der Erfolg des "Einbruchs" zum Zwecke der "kostenlosen Wissengewinnung" hängt von der Qualität der Informationen über das Zielobjekt ab.

Falls sie einen Einbruch nach der "klassischen Methode" erleben, indem ein"Mitarbeiter" oder man kann ihn auch anders nennen, so sind sie in sehr guter Gesellschaft. Ein "berechtigter Mitarbeiter" hat aus einen Sicherheitsnetzwerk der amerikanischen Regierung mehrere Gigabyte, oder auch mehr, geklaut. Über den Schaden schweigt besagte Regierungsbehörde für die Informationssicherheit der Regierungsinformationen.

Gegenmaßnahmen :

Schützen Sie alle Informationen über ihre kybernetische Einheit. Sie erschweren damit die Erfolgsmöglichkeiten bei einem Einbruch. Prahlen Sie nicht mit ihren Sicherheitssystemen. Denn es gibt immer wieder Menschen, die ihnen zeigen, dass ihr Sicherheitssystem doch "löchrig" ist.

Fortsetzung folgt !

000

Berlin, 11/ 2011

Old Gocs