AWARE7
full service awareness agency

Technicalrider

AWARE7 GmbH

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

AWARE7 GmbH

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Einleitung

Dieses Dokument ist Informationsmaterial dazu, wie Penetrationstests durch die AWARE7 GmbH durchgeführt werden. Für dieses Dokument definieren wir Penetrationstests als: "Eine Methode, um die Sicherheit eines IT-Systems zu gewährleisten, indem versucht wird, die Sicherheit dieses Systems ganz oder teilweise zu durchbrechen, wobei die gleichen Werkzeuge und Techniken verwendet werden, die einem Angreifer zur Verfügung stehen.“

Penetrationstests sollten als eine Methode zur Erlangung von Sicherheit in den Schwachstellenbewertungs- und -managementprozessen Ihres Unternehmens betrachtet werden, nicht als primäre Methode zur Identifizierung von Schwachstellen. Dies ist eher ein Nebenprodukt einer langfristig angelegten Sicherheitsstrategie.

Ein Penetrationstest sollte ähnlich wie ein Finanz-Audit betrachtet werden. Ihr Finanzteam verfolgt Ausgaben und Einnahmen täglich. Ein Audit durch eine externe Gruppe stellt sicher, dass die Prozesse Ihres internen Teams ausreichend sind und Ihre Systeme entsprechend geschützt sind, beziehungsweise Sie Bewertungs- und Managementprozesse entsprechend optimieren können.

Dieses Dokument soll Ihnen dabei helfen, die richtigen Systeme zu identifizieren und passende Verfahren und Methodiken auszuwählen. Es wird zudem dargestellt, welche Voraussetzungen nötig sind, um einen Penetrationstest bei Ihnen effizient und erfolgreich durchzuführen.

Das Dokument beginnt mit einer Auflistung von Referenzpartnern und -projekten. Im Anschluss folgen einige Erklärungen zu Penetrationstests im Allgemeinen und der angewendeten Methodik der AWARE7 im Speziellen. Daran anknüpfend werden beispielhafte Auftragsbedingungen und eine Aufwandsabschätzung beschrieben. Abschließend stellt die AWARE7 sich und Ihre Penetrationstester vor.

AWARE7 GmbH

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Referenzprojekte

Projekttyp	Kunde	Branche	Ansprechpartner	Umfang
Penetrationstest	Mittelständler	Analytics	TLP:RED	20 PT
Arbeitspakete	• Detailanalyse Webanwendung • Detailanalyse API • Detailanalyse Webseite • Externe Scans • Interne Scans			
Projektbeschreibung	Der Kunde ist eine Unternehmensberatung, die sich um Ihre Unternehmenskultur kümmert. Bringen Sie mit dem Kunden Ihre Kultur auf den neusten Stand und sorgen Sie so für nachhaltige Qualität. Der Kunde benötigte eine schnelle Lösung im Bereich Penetrationstest inklusive Nachtest für einen Kunden, den die Experten der AWARE7 GmbH gerne durchgeführt haben.			

Projekttyp	Kunde	Branche	Ansprechpartner	Umfang
Penetrationstest	Unternehmen im Medizinsektor	Medizin	TLP:RED	10 PT
Arbeitspakete	• Detailanalyse Android Anwendung • Detailanalyse API • Detailanalyse Webseite • Analyse der Datenbank • Externe Scans • Interne Scans			
Projektbeschreibung	Der Kunde vertreibt Ihr persönliches Gesundheitscockpit und eine mobile Lösung für Patienten zur Interaktion mit Gesundheitsversorgern. Der Kunde benötigte eine schnelle Lösung im Bereich Penetrationstest inklusive Nachtest, um die Sicherheit der Anwendungsdaten sicher zu stellen. Die Experten der AWARE7 GmbH haben diesen gerne durchgeführt.			

Projekttyp	Kunde	Branche	Ansprechpartner	Umfang
Umfassender Penetrationstest	Kosmetikvertrieb	Kosmetik	TLP:RED	30 PT
Arbeitspakete	• Vulnerability Assessment • Detailanalyse einer Webanwendung • Detailanalyse einer Adminanwendung • Test der SSO & AD Integration • Externe Scans • Interne Scans			
Projektbeschreibung	Der Auftraggeber aus der Kosmetik Branche ist eines der größten Netzwerk-Marketing Unternehmen in Deutschland. Täglich werden unterschiedlichste Produkte von unterschiedlichsten Händlern verkauft und versendet. Die Händlerplattform war Kernziel dieses Penetrationstests.			

Projekttyp	Kunde	Branche	Ansprechpartner	Umfang
Umfassender Penetrationstest	Technologieanbieter	Lebensmittel	TLP:RED	30 PT
Arbeitspakete	• Vulnerability Assessment • Detailanalyse einer Webanwendung • Detailanalyse einer API • Detailanalyse einer Hardwarekomponente • Externe Scans			
Projektbeschreibung	Der Auftraggeber ist Zulieferer für eine große Einzelhandelskette in Deutschland. Täglich werden unterschiedlichste Produkte von unterschiedlichsten Endkunden und Verbraucher verkauft und versendet. Die Hardware inklusive der Online Infrastruktur war Teil dieses Tests.			

Projekttyp	Kunde	Branche	Ansprechpartner	Umfang
Umfassender Penetrationstest	Technologieanbieter	Wahlsysteme	TLP:RED	10 PT
Arbeitspakete	• Vulnerability Assessment • Detailanalyse einer Webanwendung • Detailanalyse einer Serverkomponente • Externe Scans			
Projektbeschreibung	Der Auftraggeber ist ein Anbieter im Bereich der Online-Wahlsysteme. Die Software inklusive der Online Infrastruktur und einer Serverkomponente war Teil dieses Tests.			

Projekttyp	Kunde	Branche	Ansprechpartner	Umfang
Awarenesskampagne	KRITIS Versorger	Gas- & Wasserversorgung	TLP:RED	100 Vorträge
Arbeitspakete	• Vorträge zum Thema Awareness • Individuell abgestimmte Schulungsinhalte • Zielgruppenorientierte Fokusvorträge			
	Im Rahmen einer ganzjährig laufenden Awarenesskampagne wurden über 2000 Mitarbeiter einer KRITIS Infrastruktur im korrekten Umgang mit Cybergefahren geschult. Diese Kampagne wurde aufgrund des Erfolgs wiederholt durch den Kunden gebucht.			

Penetrationstests - Allgemeines

Im Folgenden werden die unterschiedlichen Informationen, Arten und Typen von Penetrationstests beschrieben und aufgeführt.

Ein Penetrationstest umfasst neben den technischen Experten eine Vielzahl von weiteren Aspekten.

Personen, die den Penetrationstest ausführen sollten über angemessene Fähigkeiten verfügen und alle fachlichen Anforderungen abdecken. Im Idealfall arbeitet der Prüfer für eine Prüfstelle mit entsprechender Expertise und verfügt über ausreichend technische Qualifikationen und Zertifikate (CEH, OSCP, OSSTMM Bachelor/Masterabschluss etc.) im Bereich IT-Sicherheit.

Im Vorfeld eines Penetrationstests werden sämtliche Rahmenbedingungen für die Durchführung des Tests festgelegt. In einem gesonderten Vertrag werden die grundlegenden Ziele des Tests erklärt sowie allgemeine Informationen zur Durchführung des Penetrationstests vereinbart. Zudem kann eine Geheimhaltungsvereinbarung zwischen beiden Vertragsparteien unterzeichnet, was den Prüfer dazu verpflichtet, keine sensitiven Informationen an Dritte weiterzugeben. Die AWARE7 verpflichtet sich und seine Analysten auf Vertraulichkeit und die Nicht-Offenlegung von Kundeninformationen und Testergebnissen. Wir empfehlen Ihnen dennoch, eine Geheimhaltungsvereinbarung abzuschließen. In weiteren Dokumenten können zudem datenschutzrechtliche Themen behandelt werden, sowie alle sonstigen Themen.

Nachdem alle rechtlichen Anforderungen für die Durchführung des Penetrationstests geschaffen wurden wird in Zusammenarbeit beider Vertragsparteien über die Festlegung der Prüfobjekte entschieden. Umgangssprachlich spricht man hier oft vom sogenannten “Scope”. Dies können beispielsweise Netzkoppelelemente wie ein Router, Switch oder Gateway sein. In den häufigsten Fällen handelt es sich jedoch um aus dem Internet erreichbare Systeme, welche auch als Webanwendungen bezeichnet werden. Bereiche der physischen Sicherheit können allerdings ebenfalls Gegenstand des Scopes sein (z.B. Zutrittskontrollmechanismen, Gebäudesteuerung etc.). Generell kann man sagen, dass es sich um Systeme handelt, die in irgendeiner Form schutzbedürftig sind.

Die Festlegung des Prüfumfangs ist ebenfalls ein elementarer Bestandteil eines Penetrationstests. Zu den wichtigsten Themen zählen hier Prüfzeitraum, Prüfbedingungen sowie Prüfort. Auch die Prüftiefe kann variieren. So kann beispielsweise vereinbart werden, dass nur bestimmte Teile einer Webanwendung getestet werden.

Beide Vertragsparteien müssen zudem Projektverantwortliche bestimmen, die als direkte Ansprechpartner im Rahmen des Penetrationstests fungieren.

Nachdem alle rechtlichen Anforderungen für die Durchführung des Penetrationstests geschaffen wurden geht der Prüfer in die Testphase über. Der Prüfer macht sich mit dem System vertraut und führt für das System angemessene Prüfungshandlungen durch. Werden dabei IT-relevante Schwachstellen identifiziert so dokumentiert der Prüfer dies entsprechend. Nach Abschluss der Testphase werden alle identifizierten Schwachstellen in einem Abschlussbericht zusammengefasst.

Testarten

Im Folgenden werden die drei unterschiedlichen Testarten beim Penetrationstest beschrieben.

Whitebox Testing

Alle Informationen über das Ziel werden der AWARE7 GmbH mitgeteilt. Diese Art von Tests bestätigt die Wirksamkeit der internen Schwachstellenbewertung und Managementkontrollen, indem sie die Existenz bekannter Software-Schwachstellen und gängiger Fehlkonfigurationen in den Systemen einer Organisation identifiziert. Da die Informationen gesichtet, bewertet und analysiert werden müssen, ist diese Art des Testings in der Regel anspruchsvoll in Bezug auf den Testzeitraum und den aufzuwendenden Aufwand.

Blackbox Testing

Es werden keine Informationen über die Interna des Zielsystems an die AWARE7 GmbH weitergegeben. Diese Art von Tests wird aus der externen Perspektive durchgeführt und zielt darauf ab, Wege zu finden, um auf die internen IT-Assets einer Organisation zuzugreifen. Dadurch wird das Risiko, dem Angreifer ausgesetzt sind, die unbekannt oder nicht mit der Zielorganisation verbunden sind, genauer wiedergegeben. Der Mangel an Informationen kann jedoch auch dazu führen, dass Schwachstellen in der für die Tests vorgesehenen Zeit unentdeckt bleiben.

Greybox Testing

Zwischen White- und Blackbox Test ist der Greybox-Test angesiedelt. Während ein Blackbox-Tester ein System aus der Sicht eines Außenstehenden untersucht, hat ein Greybox-Tester die Zugriffs- und Wissensebenen eines Benutzers, möglicherweise mit erhöhten Privilegien auf einem System. Bei einem Greybox-Test haben wir in der Regel Kenntnisse über die Interna eines Netzwerks, möglicherweise einschließlich der Design- und Architekturdokumentation und eines netzwerkinternen Accounts.

Der Zweck von Greybox-Tests ist es, eine gezieltere und effizientere Bewertung der Sicherheit eines Netzwerks zu liefern als eine Blackbox Bewertung. Mit Hilfe der Design-Dokumentation für ein Netzwerk können die Pentester der AWARE7 Ihre Bewertungsbemühungen von Anfang an auf die Systeme mit dem größten Risiko und dem größten Wert konzentrieren, anstatt Zeit mit der Bestimmung dieser Informationen zu verbringen. Ein interner Account auf dem System ermöglicht auch das Testen der Sicherheit innerhalb des gehärteten Perimeters und simuliert einen Angreifer mit längerfristigem Zugriff auf das Netzwerk.

Testtypen

Im Folgenden werden unterschiedliche Testtypen beschrieben, die entweder als Black-, White oder Greybox Test durchgeführt werden können.

Identifizierung von Schwachstellen in Ihrer Software

Am häufigsten in Webanwendungen verwendet. Diese Art von Tests muss den Entwicklern Rückmeldung über Ihre eingesetzten Programmierpraktiken geben, um entsprechende Schwachstellen zu vermeiden. Diese Tests können auf textueller Basis als Code Review durchgeführt werden oder dynamisch in Ihrer Anwendung/Ihrem System.

Szenariogetriebene Tests zur Identifizierung von Schwachstellen

Die Penetrationstester untersuchen ein bestimmtes Szenario, um herauszufinden, ob eine entsprechende Gegenmaßnahme funktioniert oder in welcher Intensität das System beeinträchtigt werden kann. Die Szenarien können sein: Verlorener Laptop, nicht autorisiertes Gerät, das mit dem internen Netzwerk verbunden ist oder ein kompromittierter DMZ-Host. Es gibt allerdings viele andere mögliche Szenarien. Sie sollten, basierend auf früheren Vorfällen, überlegen, welche Szenarien für Ihre Organisation am relevantesten sind und entsprechende Penetrationstests durchführen lassen.

Szenariogetriebene Tests der Erkennungs- und Reaktionsfähigkeit

Bei dieser Version der szenariogesteuerten Tests geht es darum, die Erkennungs- und Reaktionsfähigkeit Ihrer Organisation zu bewerten. Dies wird Ihnen helfen, die entsprechende Wirksamkeit und Abdeckung im jeweiligen Szenario zu verstehen.

Mögliche Schwachstellen, die im Rahmen eines Penetrationstests auftreten können

Im Folgenden werden mögliche Schwachstellen dargestellt, die im Rahmen eines Penetrationstests gefunden werden können. Sie reicht von unberechtigtem Datenabfluss, über Berechtigungsmanagement bis hin zum Parameter-Fuzzing. Wir orientieren uns dabei entweder an offenen Standards, beispielsweise OWASP Top 10 oder dem OSSTMM. Aufgrund von Gegebenheiten individueller Anwendungen kann es sein, dass von diesem Katalog beziehungsweise von einzelnen Modulen abgewichen wird. Die Schwachstellen werden mit Hilfe von CVSS kategorisiert und in den Report

aufgenommen. Es werden, in Abhängigkeit des betrachteten Systems, unter anderem folgende Schwachstellen überprüft:

Schwachstelle	Erklärung
Cross Site Scripting	Cross Site Scripting (XSS) bezeichnet einen Angreifer, der aktive Inhalte auf das Zielobjekt schreibt und diese dann an einen Anwender weitergeleitet werden. Der Browser des Anwenders erkennt diesen Code nicht als Fremdcode und führt diesen aus. Angreifer nutzen dies aus, um beispielsweise an Authentisierungsmerkmale des Benutzers zu kommen oder sog. Drive-By Infektionen durchzuführen.
Cross Site Request Forgery	Wenn eine Webanwendung nicht überprüft, ob Anfragen durch einen legitimen Nutzer-Request (bspw. Klick) oder anders generiert wurden, bietet sich die Möglichkeit eines CSRF. Dies wird häufig genutzt um unvorsichtige Nutzer dazu zu bringe, dass Sie Datensätze löschen oder komplexere Prozesse anstoßen.
SQL-Injection	Ein erfolgreicher SQL-Injection Angriff führt zu einem Zugriff und auslesen von Daten aus einem Web-Portal. Je nach Konfiguration können einzelne Werte, Spalten/Zeilen oder ganze Tabellen betroffen sein. Angriffsvektor ist User Input, beispielsweise bei Formfeldern.
Cookie Analysen	Cookies managen Sessions eines Nutzers. Wird ein Cookie nicht ausreichend randomisiert generiert wird, kann ein Angreifer einen passenden Cookie erraten und sich so Zugang zur Plattform verschaffen, ohne sich jemals zu authentifizieren.
Parameter Fuzzing	Bei der Nutzung eines Portals versenden Anwender unterschiedliche Parameter über POST/GET oder sonstige Befehle. Ist kein Fehlerhandling oder nur unzureichendes Handling implementiert kann dies zur Ausführung von Code außerhalb der Grenzen des Portals führen. Ein Angreifer kann dafür sorgen, dass einzelne Komponenten versagen oder sich Zugang zu anderen Systemen verschaffen. Wenn Kommandos injiziert werden können, kann dies zu weiterem Informationsabfluss führen.
Business Logik	Lassen sich Parameter so variieren, dass Änderungen im Programmablauf oder der Prozesslogik erzielt werden können, wodurch ein Abfall der Sicherheit zu verzeichnen ist.
System Takeover	Das System lässt sich komplett übernehmen und es können andere Ressourcen gesteuert und beeinflusst werden.
OSINT	Open Source Intelligence (OSINT) ist eine Recherchetechnik. Im Rahmen der Recherche werden frei verfügbare Datensätze und Netzwerke nach Informationen zum Unternehmen und zu Mitarbeitern durchsucht. Diese Informationen werden im weiteren Verlauf wichtig, um maßgeschneiderte Phishing E-Mails zu versenden oder einen leichten Zugang zum Unternehmen zu ermöglichen.
Smishing/ Vhishing/ Phishing	Beim Phishing wird eine E-Mail im Namen eines Anderen gesendet und es wird versucht einen Mitarbeiter zur Preisgabe vertraulicher Informationen zu bewegen oder Schadcode auf dem Rechner zu platzieren. Beim Smishing und Vishing ist der Angriffsvektor keine E-Mail, sondern eine SMS beziehungsweise ein Telefonanruf.
Peripherie	Kann im physikalischen Umfeld des Unternehmens ein anderer Angriffsvektor gefunden werden? Gibt es interne Netzwerke, die über unzureichende Authentifizierungsmechanismen verfügen, auf die von außen zugegriffen werden kann?
Fake Access Points	Klonen der verfügbaren Netzwerke in der Nähe des Unternehmens und versuch an Login-Daten der Mitarbeiter zu kommen über Access-Point-Phishing. Das freie WLAN der Angreifer verlangt eine Authentifizierung mit den Unternehmensdaten.
Impersonation Attack	Ein Berater der AWARE7 GmbH wird versuchen sich mit Hilfe einer anderen Identität, beispielweise aus der Supply Chain oder dem Dienstleistungsumfeld des beauftragenden Unternehmens, Zugang zum Unternehmen zu verschaffen. Dort wird er dann versuchen sich Zugang zu IT Systemen zu verschaffen, beispielsweise über USB-Sticks oder das Netzwerk

Die Dokumentation der Angriffe erfolgt mit einem strukturierten Report. Da es nur beschränkt offizielle Richtlinien, Guidelines o.ä. gibt, ist jeder durchgeführte Angriff teilweise einzigartig in Vorbereitung, Verlauf und Berichterstattung. Handlungsempfehlungen und Vermeidungsstrategien eingeschlossen.

Diese Liste erhebt keinen Anspruch auf Vollständigkeit und dient nur zur Orientierung für den Kunden.

Penetrationstest einer Cloud Anwendung

Es gibt zunehmend eine erhöhte Anzahl an Cloud Anwendungen, welche ebenfalls einem Penetrationstest unterzogen werden können. Vorranging sind hier Amazon Web Services und Azure von

Microsoft zu nennen. Diese Anwendungen können ebenfalls einem Penetrationstest unterzogen werden.

Sollten Sie dies in Erwägung ziehen denken Sie daran, dass beide Plattformen Pentests generell erlauben, es allerdings Einschränkungen gibt.

Penetrationstest einer Mobilen Anwendung

Heutzutage verarbeiten auch mobile Anwendungen häufig sensible Daten und werden damit zum Hauptziel von Cyberkriminellen. Bei der Arbeit mit solchen Daten müssen alle am Entwicklungsprozess beteiligten Personen den Schutz der Applikation gewährleisten. Ein Penetrationstest erhöht die Sicherheit von mobilen Anwendungen in der Regel deutlich.

Eine Android Applikation lässt sich in der Regel ohne große Probleme testen, da sich eine „.apk"-Datei ohne viel Aufwand in Quellcode überführen lässt. Sollten Sie ein Quellcode Review wünschen und Ihre Applikation obfuskieren ist es im Sinne eines ressourceneffizienten Penetrationstest uns den Quellcode zur Verfügung zu stellen. Bei einer iOS Applikation müssen Sie als Auftraggeber im Besitz der „.ipa"-Datei sein, damit wir Zugriff auf den Quellcode haben und Ihre Applikation testen können.

Grenzen eines Penetrationstests

Sicherheitstests stellen immer nur Analysen des „IST-Zustands" dar. Mögliche zukünftige Konfigurationsänderungen oder Ablaufänderungen werden nur schwer fassbar im Penetrationstest und sind eher Spekulation als greifbare Realität. Damit Sie das meiste aus unseren Penetrationstests rausholen, sollten Sie diese regelmäßig durchführen und Sicherheit als Prozess implementieren.

Ein weiteres Hemmnis ist häufig das Budget. Werden komplexe Applikationen oder Netzwerke in einem kurzen Zeitraum geprüft, besteht ein Risiko, dass Sicherheitslücken aus zeitlichen Gründen nicht gefunden werden können. Ein Angreifer hat theoretisch gesprochen „unendlich" viel Zeit Sie und ihr Unternehmen zu beobachten und kann tiefgehend Untersuchungen einleiten und dadurch neue Sicherheitslücken aufdecken und ausnutzen.

Planung eines Pentest-Projektes

Wenn die Durchführung eines Penetrationstests frühzeitig terminiert wird ist die Planung und Durchführung nicht schwer. Zwar ist die AWARE7 auch in der Lage kurzfristige Penetrationstests durchzuführen, jedoch erzeugt dies immer einen vermeidbaren Mehraufwand. Selbst ein kompakter Test ist im Sinne der IT-Sicherheit besser, als gänzlich zu verzichten.

Eingesetzte Methodik und Ablauf

Ein typischer Penetrationstest durch die AWARE7 folgt diesem Muster: Kick Off, Recon Phase, Enumeration, Vulnerability Identification, Exploitation, Post Exploitation, Reporting. Es sollte eine Einstufung des Schweregrades für alle gefundenen Probleme erfolgen.

Bei diesem Modell gehen wir davon aus:

- Sie möchten wissen, welche Auswirkungen ein Angreifer hat, der eine Schwachstelle ausnutzt, und wie wahrscheinlich es ist, dass sie auftritt
- Optimal: Sie haben einen internen Schwachstellenbewertungs- und -managementprozess

Erstes Engagement unseres Teams

Sie sollten sicherstellen, wenn Sie ungewöhnliche Systeme haben (Mainframes, ungewöhnliche Netzwerkprotokolle, maßgeschneiderte Hardware usw.), dass uns diese im Angebotsverfahren hervorgehoben werden, damit unsere Tester und wir wissen, welche Fähigkeiten und Ressourcen erforderlich sind.

Kick Off

Im Rahmen der Gespräche vor dem Kick Off und dem Kick Off Termin selbst, vereinbaren wir einen Scope. An diesem Kick Off sollten folgende Personen aus Ihrem Unternehmen teilnehmen:

- Alle relevanten Risiko- oder Produkteigentümer
- Technisches Personal mit Kenntnissen über das Zielsystem

Wenn Sie schon ein Schwachstellenmanagement haben, sollten Sie folgende Themen vorbereiten:

- Die Risikoeigentümer sollten alle Bereiche von besonderem Interesse skizzieren
- Das technische Personal sollte die technischen Grenzen der IT-Abteilung des Unternehmens umreißen.

Folgende Themen werde im Rahmen des Kick Off Gesprächs von uns gemeinsam mit Ihnen definiert oder abgesprochen:

- Testzeitraum und Zeitfenster
- Besprechung des Testgegenstands
- Notwendige Voraussetzungen
- Allgemeine Hinweise zur Durchführung
- Ansprechpartner und deren Erreichbarkeit

Recon

Unter Recon oder auch Aufklärung versteht man die Arbeit der Informationsbeschaffung, bevor ein echter Angriff durchgeführt wird. Die Idee ist, so viele interessante Informationen wie möglich über das Ziel zu sammeln. Um dies zu erreichen, werden viele verschiedene, öffentlich zugängliche Informationsquellen genutzt. Die extrahierten Informationen erlauben oft schon einen detaillierten Einblick in die betroffenen Systeme.

Enumeration und Vulnerability Identification

In der Enumerationsphase werden mögliche Einstiegspunkte in die getesteten Systeme identifiziert. Die während der Recon Phase gesammelten Informationen werden hier genutzt.

Während der Enumeration werden systematisch Informationen gesammelt und einzelne Systeme identifiziert. Die Pentester untersuchen die Systeme in ihrer Gesamtheit. Dies ermöglicht die

Bewertung von Schwachstellen, die nicht unbedingt auf ein technisches Problem zurückzuführen sind. Ein technisch sicherer Passwortschutz kann sich z.B. als wertlos erweisen, wenn Angreifer die Passworteingabe eines Benutzers durch ein Fenster sehen können. Bei der Enumeration sammeln die Pentester Informationen über mögliche Schwachstellen, die in der Ausbeutungsphase verifiziert oder widerlegt werden.

Exploitation

In der Exploitation Phase, versuchen die Penetrationstester Sicherheitsschwachstellen aktiv auszunutzen. Exploits werden entwickelt, um z.B. sensible Informationen zu sammeln oder um es den Pentestern zu ermöglichen, ein System zu kompromittieren und sich darauf zu manifestieren. Ist ein System einmal erfolgreich kompromittiert, ist es oft möglich, in weitere Systeme einzudringen, da die Pentester nun Zugang zu mehr potentiellen Zielen haben, die vorher nicht verfügbar waren, z.B. weil das kompromittierte System in der Lage ist, mit internen Systemen zu interagieren, die nicht vom Internet aus zugänglich sind. Bei neuen Zielen werden die Aufklärungs- und Enumerationsphasen erneut durchlaufen, um Informationen über diese neuen Systeme zu sammeln und diese auch auszunutzen.

Post Exploitation & Report

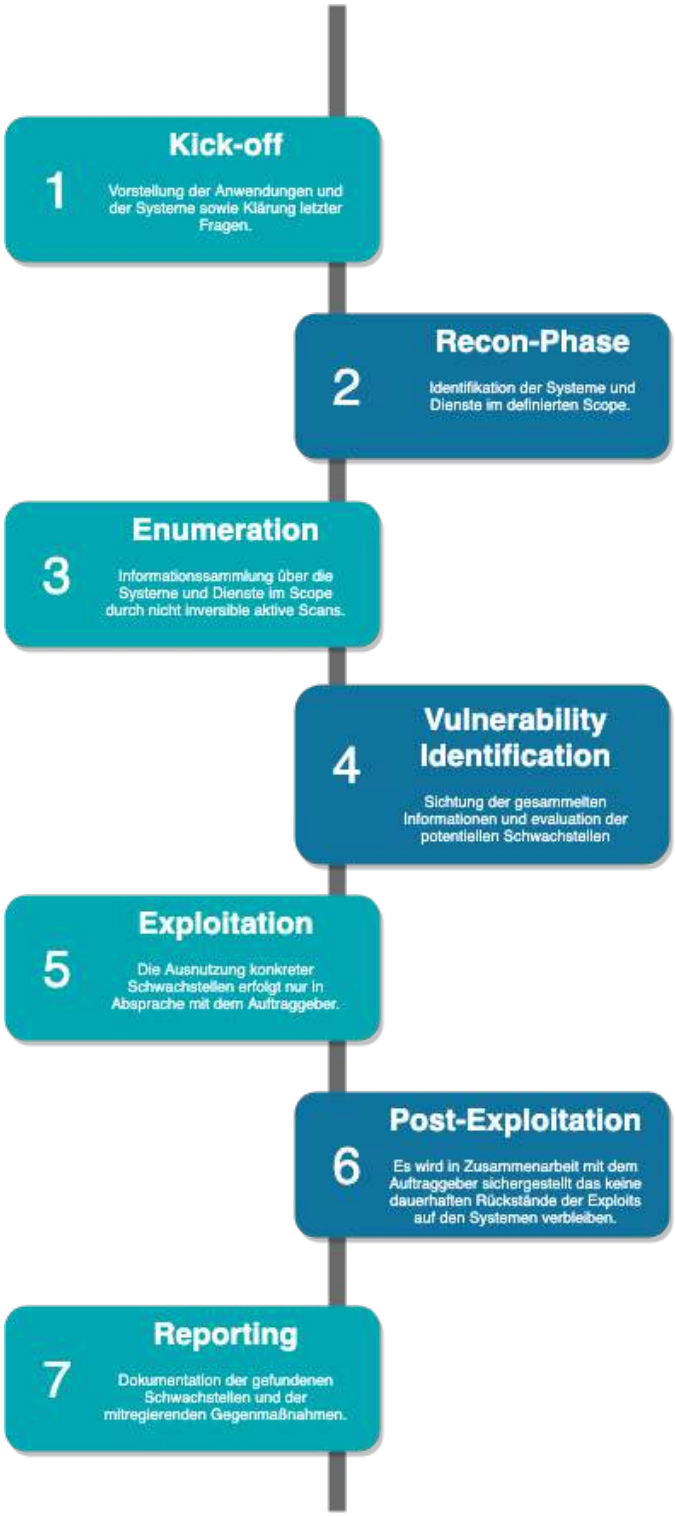
Die Dokumentation ist ein wesentlicher Bestandteil jedes Penetrationstests. Während des Penetrationstests werden alle Schritte, die zu einem erfolgreichen Angriff führen, ausführlich dokumentiert. So ist sichergestellt, dass nach dem Test alles im Detail nachvollzogen werden kann. Am Ende des Penetrationstests dient diese Dokumentation als Grundlage für einen individuellen Bericht, der die Testergebnisse sowohl für die technische Administration als auch für das Management nachvollziehbar macht. Der Seitenumfang eines solchen Berichtes liegt in der Regel im zwei bis dreistelligen Bereich und umfasst folgende Punkte:

- Alle aufgedeckten Sicherheitsprobleme
- Eine Bewertung durch das Testteam hinsichtlich des Risikoniveaus, dem jede Schwachstelle die Organisation oder das System aussetzt
- Eine Methode zur Lösung jedes gefundenen Problems
- Eine Nachbesprechung kann ebenfalls nützlich sein. Bei diesem Treffen geht das Testteam seine Ergebnisse durch und Sie können weitere Informationen oder die Klärung von Fragen anfordern.

Der gesamte Bericht wird von den Penetrationstestern, die die Prüfung durchgeführt haben, erstellt, damit die Dokumentation die Ergebnisse optimal abdeckt und alle wichtigen Details zu den einzelnen Befunden enthält. Nach der Exploitation und während der Reportphase wird zudem in Zusammenarbeit mit Ihnen sichergestellt, dass keine Systeme mehr durch Exploits beeinträchtigt sind.

Beim Reporting kategorisieren wir gefundene Schwachstellen in entsprechenden Kategorien „niedrig“, „mittel“, „hoch“ oder „kritisch“. Bei Bedarf kategorisieren wir die gefundenen Schwachstellen gerne genau numerisch nach dem Common Vulnerability Scoring System (CVSS). Von uns gefundene Schwachstellen werden normalerweise auf einer dieser Ebenen einheitlich kategorisiert, können allerdings manchmal auch aus diesem Muster ausfallen. Beispielsweise könnten andere Kontrollen die Wirksamkeit einer Schwachstelle minimieren, oder das Vorhandensein zusätzlicher Schwachstellen könnte einen Synergieeffekt haben. Jede Abweichung von der Zuordnung einer Schwachstelle zu ihrer Standardbewertung wird von uns dokumentiert und begründet.

AWARE7
full service awareness agency



AWARE7 GmbH

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Ihre Ansprechpartner

Herr Matteo Große-Kampmann ist Ihr zentraler Ansprechpartner für alle Rückfragen zu diesem Angebot. Herr Moritz Gruber ist zudem der fachliche Projektleiter während der Umsetzung.

	Matteo Große-Kampmann Geschäftsführer	Moritz Gruber Fachlicher Projektleiter
Adresse	Munscheidstraße 14 45886 Gelsenkirchen	Munscheidstraße 14 45886 Gelsenkirchen
Telefon	+49 209 88306762	+49 209 88306765
Mobil	+49 15739446386	+49 209 88306765
E-Mail	matteo@aware7.de	moritz@aware7.de

Qualitäts- und Risikomanagement

Herr Matteo Große-Kampmann ist Ihr zentraler Ansprechpartner für alle Fragestellungen zur Leistungserbringung der AWARE7. Er wird projektübergreifende Aspekte in seiner Aufgabe als Gesamtverantwortlicher wahrnehmen und stellt Eskalationskontakt, sowie Qualitätsverantwortlichen dar.

Herr Moritz Gruber ist für die Leitung und Steuerung der operativen Tätigkeiten im Projekt verantwortlich. Er stellt sicher, dass die Spezialisten optimal eingesetzt werden und steuert projektbezogene Aspekte. Er trägt Sorge, dass alle zu verrichtenden Arbeiten reibungslos umgesetzt werden. Er steht für die hohe Qualität der AWARE7 GmbH ein und wird die erforderlichen Entscheidungen zeitnah und zielführend treffen.

Projektteam

Unser Team setzt sich aus erfahrenen Mitarbeitern zusammen, die viele Jahre und auf unterschiedliche Arten Projekte in Unternehmen und an Universitäten betreut haben. Für das Projektteam werden erfahrene Mitarbeiter mit fundierter Ausbildung und mehrjähriger Berufserfahrung eingesetzt. Sie verfügen über die notwendige Branchenexpertise. Die eingesetzten Analysten werden durch das AWARE7 Backoffice sowie andere Projektteams unterstützt, um den Transfer unterschiedlicher Kompetenzen sicherzustellen. Das Team ist nicht fest zusammengesetzt, sondern wird im Rahmen der Projektanforderungen dynamisch zusammengestellt, so kann bei Bedarf auf das gesamte Know-How der AWARE7 zugegriffen werden. Die möglichen Penetrationstester sind im Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** aufgeführt.

Über die AWARE7 GmbH

Die AWARE7 GmbH ist ein Cyber Security Unternehmen aus Gelsenkirchen das Technologien und Produkte entwickelt sowie Dienstleistungen anbietet, die zur Förderung, Steigerung und Erhaltung des IT-Sicherheitslevels dienen. Durch die praktische Arbeit und der regelmäßigen Veröffentlichung von wissenschaftlichen Artikeln gelingt es uns komplexe Betrugs- und Angriffsmethoden zu erklären um Unternehmen, Behörden und Personen zu schützen.

IT-Sicherheit funktioniert nur, wenn die Technik sicher und die Menschen sensibilisiert sind. Komplexe Angriffe nutzen menschliche Schwachstellen in Kombination mit technischen Sicherheitslücken aus. Betrachten Sie das IT-Sicherheitsniveau in Ihrem Unternehmen ganzheitlich. Auf menschlicher und technischer Ebene.

Portfolio

Live Hacking

& Awareness Shows

Bei einem Live Hacking geht es darum, die Risiken kennenzulernen, welche im Umgang mit bewährten und neuen digitalen Medien entstehen. Ein Live Hacking kann sich über unterschiedliche Zeiträume erstrecken. Bei allen Vorträgen geht es darum, den Stand der IT-Sicherheit darzustellen, denn wer sich vor Angriffen, Sicherheitslücken und Betrugsmaschen schützen will, muss wissen wie die Kriminellen vorgehen. Dabei soll nicht vor der Digitalisierung abgeschreckt werden. Teilnehmer erhalten viel mehr die Möglichkeit sich und andere zu schützen.

Phishing Kampagnen

& Social Engineering Audits

Die meisten Angreifer erhalten über eine Phishing Mail Zutritt zum Unternehmen. Dabei sind es nicht die schlechten Phishing Mails, die für das Unternehmen zur Gefahr werden. Es sind perfektionierten Mails, von denen die Opfer gar nicht merken, dass sie auf eine Phishing Mail hereingefallen sind. Um Ihr Unternehmen vor dem beliebtesten Einfallstor zu schützen, Ihre Mitarbeiter zu trainieren und weiterzubilden, führen wir Phishing Kampagnen auf unterschiedlichen Erkennungsniveaus durch.

Penetrationstest

von Web, iOS und Android Applications

Ein Penetrationstest hat zum Ziel technische Sicherheitslücken einer oder mehrerer bestimmter Anwendungen aufzudecken. Im Anschluss an die Risikobewertung sollte die Gefahr minimiert oder bestenfalls geschlossen werden. Wir untersuchen ihre Infrastruktur, Web, iOS oder Android Application auf Sicherheitslücken, dokumentieren diese sorgfältig, fertigen individuelle Handlungsempfehlungen an und präsentieren den Bericht auf Wunsch vor Ort. Dieser Test erfolgt in den meisten Fällen auf einem Testsystem und wird, um das System widerstandsfähig gegenüber Angreifern zu machen, regelmäßig wiederholt.

RiskRex

Digital Risk Management

Moderne Angriffe nutzen menschliche & technische Sicherheitslücken meist in Kombination. RiskRex hilft Ihnen dabei, das IT-Sicherheitsniveau in Ihrem Unternehmen ganzheitlich zu betrachten und Gegenmaßnahmen einzuleiten. RiskRex hilft Ihnen, das Risiko von Mitarbeiterinnen, Mitarbeitern und der technischen Infrastruktur im Unternehmen zu messen.

AWARE7 GmbH

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Anhang

Mitgliedschaft in Verbänden

Um die Rolle der AWARE7 GmbH im IT-Sicherheitsbereich weiter zu verstärken, stehen wir im ständigen Austausch mit relevanten Unternehmen, Organisationen und Forschungseinrichtungen. Darüber hinaus engagiert sich die AWARE7 GmbH in Vereinen und Verbänden, die sich der Weiterentwicklung von IT-Sicherheitslösungen und Konzepten widmen.

eco - **Verband der Internetwirtschaft e.V.**	Mit der Digitalisierung erleben wir eine Phase des Strukturwandels und des Umbruchs, in der sich traditionelle Industrie- und Wirtschaftsbereiche verändern, täglich neue Geschäftsmodelle entstehen und bestehende digitale Anwendungen optimiert werden. Das Internet verändert unser Kommunikationsverhalten, unsere Arbeitsweise, unseren gesamten Alltag. Es verändert auch die Wirtschaft fundmental – und damit jedes einzelne Unternehmen. Das eco Hauptstadtbüro versteht sich als Sprachrohr der Internetbranche im politischen Berlin und in Brüssel. Dafür bringt unser interdisziplinäres Team aus Juristen, Politikwissenschaftlern und PR-Fachleuten seine gesamte Kompetenz ein.
eurobits **Europäisches Kompetenzzentrum** **für IT-Sicherheit**	Mit eurobits e. V. hat sich seit 1999 erfolgreich eine Dachmarke etabliert, unter der sich führende Forschungsinstitute, engagierte Unternehmen der Branche sowie junge Wachstumsunternehmen vereint haben. Jedes Mitglied bringt einen enormen Schatz an wertvollem Spezialwissen aus dem Bereich der IT-Sicherheit und Informationssicherheit mit. Damit ist eurobits der kompetente Ansprechpartner für Anfragen zu aktuellen IT-Sicherheitsthemen mit technologischem, wirtschaftlichem und wissenschaftlichem Bezug. eurobits hat auch ein vielgefächertes Angebot an wissenschaftlichen Studiengängen und zertifizierten Weiterbildungsangeboten, welches in seiner Breite einzigartig in Deutschland ist. Die eurobits Mitglieder bieten u.a. die folgenden Studien- und Weiterbildungsmöglichkeiten an.
ASW **Allianz für Sicherheit in der Wirtschaft** **Nordrhein-Westfalen e.V.**	Die Allianz für Sicherheit in der Wirtschaft e.V. versteht sich als eine branchenübergreifende Plattform für einen Informationsaustausch zu sicherheitsrelevanten Herausforderungen der Privatwirtschaft. Durch ein umfangreiches Portfolio an Leistungen fördert der Verband die Kriminalprävention. Zu unseren Mitgliedern zählen Großkonzerne, kleine und mittelständische Unternehmen sowie Unternehmen der Sicherheitswirtschaft. Der Verband ist Mitglied der Public-Private Partnership „Sicherheitspartnerschaft NRW gegen Wirtschaftsspionage und Wirtschaftskriminalität“, zusammen mit den Landesministerien des Inneren und der Wirtschaft sowie der IHK NRW. Dabei verfolgt die ASW West - Allianz für Sicherheit in der Wirtschaft West e.V. ausschließlich und unmittelbar gemeinnützige Zwecke.
Allianz für Cybersicherheit	Mit der 2012 gegründeten Allianz für Cyber-Sicherheit verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. 133 Partner und 97 Multiplikatoren engagieren sich im Rahmen der Initiative und leisten so einen wertvollen Beitrag für mehr Cyber-Sicherheit am Wirtschaftsstandort Deutschland.
Bundesverband **mittelständische Wirtschaft**	Digitalisierung und Globalisierung stellen den Mittelstand vor neue gewaltige Herausforderungen. Der BVMW ist der Partner für die Unternehmen auf ihrem erfolgreichen Weg in die Zukunft. Denn der Unternehmer als Einzelkämpfer hat keine Chance mehr, gefragt sind Vernetzung und ganzheitliches Denken. Als wichtigster Mittelstandsverband Deutschlands vertritt er machtvoll die Interessen der mehr als drei Millionen Klein- und Mittelbetriebe in unserem Land. Der BVMW ist Kritiker und Partner der Politik zugleich.

AWARE7 GmbH

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Accelerator & Inkubator Programme

Die AWARE7 GmbH ist ein Unternehmen am IT-Sicherheitsmarkt und hat in der jungen Unternehmensgeschichte bereits zahlreiche Unternehmen, Organisationen, Behörden, Ministerien und Vereine von der eigenen Kompetenz überzeugen können. Für die ständige Weiterentwicklung von Sicherheitslösungen haben wir bereits an zahlreichen Accelerator & Inkubator Programmen teilgenommen.

TECHBOOST STARTUP Ein Programm der T	TechBoost, das Startup-Programm der Deutschen Telekom, unterstützt ausgewählte Technologie-Startups mit Guthaben für das Public-Cloud- Angebot der Telekom, die Open Telekom Cloud, sowie Kontakten zu potentiellen Kunden und gemeinsamen Aktivitäten im Bereich Vertrieb und Marketing. Startups mit einer digitalen Geschäftsidee auf Cloud-Basis können sich für TechBoost bewerben. Dabei spielt es zunächst keine Rolle, in welchem Entwicklungsstadium sich die Startups befinden. Denn es gibt unterschiedliche TechBoost-Programme für die verschiedenen Entwicklungsstufen.
Deutsche Telekom AG	

pwc	Scale | FinTech ist ein Programm für wachstumsstarke europäische Start-ups u. a. aus den Bereichen Banking, Financial Solutions, Kreditvergabe, digitale Vermögensverwaltung und Kryptowährung und viele weitere Themen. Wir helfen Euch über einen Zeitraum von zwei Monaten eure Skalierungshürden zu überwinden und bringen Euch mit einflussreichen Unternehmen und Investoren zusammen. Potenzielle Unternehmenskooperationen und der Austausch von wertvollem Wissen mit Branchenexperten sind nur einige der vielen Chancen, die die Teilnahme an unserem Programm bietet. Das Programm beinhaltet mehrere Bausteine, die Euer Geschäft schnell auf das nächste Level bringen. Während der Events habt Ihr als Gründer die Möglichkeit, ein großes Netzwerk aus Führungskräften und Entscheidungsträgern der Industrie kennenzulernen und Euer Business den ausgewählten PwC Kunden vorzustellen. In unseren Masterclasses bekommt Ihr von PwC und Industrieexperten essenzielles Wissen vermittelt und profitiert von individueller Hilfestellung, die auf die Bedürfnisse Eures Start-ups zugeschnitten ist.
PricewaterhouseCoopers GmbH	

PARTICIPANT CUBE 5 LIFTOFF	Das Liftoff ist ein intensives Trainingsprogramm für early stage Cybersecurity Startups. Bei dem Programm geht es um mehr als finanzielle Unterstützung. Wichtiger ist, dass jedes Startup einen kraftvollen Schub für das Geschäftsmodell erhält. Coaches und Mentoren unterstützen die Startups bei der Entwicklung ihrer Go-To-Market-Strategie und schulen sie in effektiven Kommunikationsfähigkeiten. Auf der ITS.Connect, Deutschlands größter Jobmesse für Studierende der IT-Sicherheit, bekommen unsere Liftoff-Teams die Möglichkeit, ihr Unternehmen und offene Stellen zu präsentieren. Die Startups vernetzen sich und rekrutieren ihre zukünftigen Angestellten an ihrem eigenen Messestand. In den letzten Wochen des Liftoff-Programms werden Pitch-Fähigkeiten mithilfe der Experten erlernt. Daraufhin präsentiert ihr euch bei unserem Investoren-Pitch.
Cube 5 / Ruhr-Universität Bochum	

AWARE7 GmbH

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

TV, Radio & Interviews

TV

Titel	Veröffentlicht
Gesundheit digital?	Wissenschaftsdoku, 3Sat
Sicherheit von Patientendaten - Der Preis der digitalen Medizin	ZDF heute, ZDF
Statement zum Datendiebstahl zahlreicher Prominenter und Politiker	Taff, Prosieben
Digitale Sicherheit betrifft am Ende uns alle!	WDR, Aktuelle Stunde
Live Interview zum Thema: Open Data & Sicherheit	WDR, Lokalzeit Duisburg
Live Interview zum Thema: Breitbandausbei in Essen	WDR, Lokalzeit Ruhr
Neues Facebook-Löschzentrum in Essen vorgestellt	WDR, Aktuelle Stunde
Betrug mit der 110	WDR, Lokalzeit Ruhr
Freie Ausfahrt – WannaCry betrifft Parkhäuser!	WDR, Lokalzeit Ruhr
Erpressung ála Hollywood in Essen	Frühstücksfernsehen, Sat.1
Live Interview zum Thema: Fehlinformationen im Internet	WDR, Lokalzeit Ruhr
Wie schütze ich meinen Router?	Sat. 1 NRW

Radio

Titel	Veröffentlicht
Die unsichere Kommunikation mit anonymen Quellen	Deutschlandfunk
Hackerangriff: Experten diskutieren Stromausfall im Ruhrgebiet	WDR
Services im Darknet	Radio Emscher Lippe
Hacker-Angriffe: Droht uns der totale Stromausfall?	Radio Essen
Spionageschutz	TopFM 106,4
Der ThyssenKrupp Hack	Deutschlandfunk
Payback Punkte weg, warum?	Radio Oberhausen
Anstieg von Spam in Deutschland stark gestiegen.	Antenne 1 Stuttgart

Interviews

Titel	Veröffentlicht
48 Stunden Stromausfall – Mülheim hätte ein ernstes Problem	WAZ plus
Browser synchronisieren: Wie es geht, was Sie beachten müssen	Techbook.de, hna.de
Firefox blockiert Ton und Videos Standardmäßig	Insuedthueringen.de
Wenn der eigene Körper zum Passwort wird	Saarbrücker Zeitung
Schüler lernen sich und das Netz beherrschen	Stuttgarter Nachrichten
Beim „Live Hacking“ wird’s still	Techbote
Für wen taugt Linux?	Wiesbadener Kurier
Sind Apple-Rechner sicherer als Windows-PCs?	Welt.de
NetzDG: Weniger Hass oder weniger Meinungsfreiheit?	NRW
Ist das heimische WLAN mittlerweile sicher?	Welt.de
Fingerabdruck, Iris- und Gesichtserkennung – Was kann Biometrie?	wired
Bluetooth Sicherheitslücke – Fünf Milliarden Geräte gefährdet	tagesschau
Gastkommentar: Facebook will Gedanken lesen!	Weser Kurier
Passwörter: So schützen Sie ihre Online-Accounts	Gmx.at
So ist das Bankkonto vor Hacker-Angriffen sicher!	Aachener Nachrichten
Das digitale Klassenzimmer	WAZ
Umsicht oder Virenscanner – Androiden angemessen schützen!	Gelnhäuser Tageblatt
Navigation ohne Internet, offline zum Ziel	Süddeutsche Zeitung
Die Gefahr durch Bloat- und Crapware!	Welt.de, Handelsblatt.de

Die größetn Bedrohungen im Netz	DPA
Passwörter sind sicherer als biometrische Verfahren	DPA

Fachartikel, Paper & Studien

Titel	Veröffentlicht
GDPiRate – Stealing Your Personal Information on and Offline	ESORICS 2019, Luxembourg.
Verwendung von Geolokationsdaten als Angriffsvektor für Social Engineering	DACH Security Konferenz 2018, syssec Verlag 2018
MENSCHpunktNULL - Gestaltungsansätze für die digitale Gesellschaft	Self-publishing
Kompass IT-Verschlüsselung Orientierungs- und Entscheidungshilfen für kleine und mittlere Unternehmen	Bundesministerium für Wirtschaft und Energie
Security and Privacy in Blockchain Environments	Dotmagazine
3D-Druck in der Entwicklung, Revolution des Druckens	IT-SICHERHEIT
Cybersicherheit für vernetzte Anwendungen In der Industrie 4.0	Vogel Fachverlag
Internet of Things - Herausforderungen für die IT-Sicherheit	IT-Sicherheit
Interconnected, Secured and Authenticated Medical Devices	Springer International Publishing SSIC17, Jaipur, India
Monitoring des Wohlergehens von alleinlebenden Senioren auf Basis von dezentral gemessenen Energieverbrauchswerten	VDE Kongress
Effiziente und sichere Behördenkommunikation	DATAKONTEXT-Fachverlag
Sicherheitsarchitektur von Windows 10: Sicherheitsanalyse von Windows 10 gegenüber Windows 8.1 und Windows 7	Springer Verlag
Prototyping a Minimally Invasive, Privacy-Compliant, Distributed AAL-System	IEEE Wireless Communications and Networking Conference Workshops