CYBEReinhardt

INFORMATION SECURITY SERVICES

CYBERReinhardt GmbH – Industriestr. 29-31 – D-82194 Gröbenzell

Gröbenzell, den 02.10.2021

TWIMC

1. Über die CYBEReinhardt GmbH

Dienstleistungen, Beratungen und Schulung im Bereich der offensiven Cyber- und Informations-Sicherheit, insbesondere zur Webanwendungs-Sicherheit (inkl. mobile/rich Clients und API/WS). Soforthilfe bei der Bewältigung von sicherheitskritischen Ereignissen (Incident Response).

CYBEReinhardt GmbH
Industriestr. 31
D-82194 Gröbenzell

Telefon: 08142-4100-340 Fax: 08142-4100-599
Threema: CCKFMBMW Web: www.CYBEReinhardt.de (//TODO, Baustelle)
E-Mail: Info@CYBEReinhardt.de

Alle persönlichen und funktionalen E-Mailadressen unterstützen Verschlüsselung mit GPG und S/MIME. Weiterhin unterstützen wir Dateiverschlüsselung via GPG, Veracrypt, PDF und ZIP.

1.1. Generelles Portfolio

- Penetration Testing, sowohl Mobile und Web Application Security als auch Netzwerkebene
- Incident Response und Incident Handling
- Hilfe bei Ransomware-Angriffen und Malware Analyse
- Digitale Forensik, sowohl im Notfall vor Ort als auch gerichtsverwertbar im Labor
- Red Teaming, Physical Security und Social Engineering
- Live Hacking und Awareness
- Source Code Analysen und Secure Code Reviews
- Reverse Engineering
- Audits und Assessments
- Guidelines und Policys
- Schulungen und Workshops

1.2. Notfall-Hotlines

1.2.1. Bestandskunden mit Retainer

00800-INCIDENT

Montag bis Freitag (ohne Feiertage) von 9:00 Uhr – 17:00 Uhr

Kostenfrei vom Festnetz oder Mobil aus D-A-CH und Lux

1.2.2. Neukunden, Kunden ohne Retainer oder 24/7/365-Anfragen

0900-1-INCIDENT

EUR 2,99 / Minute aus dem Festnetz, Mobilfunk abweichend (nur aus Deutschland erreichbar)

1.3. Firmenleitung

Ralf Reinhardt

Dipl.-Inf.(FH), CISM, CISSP, GWAPT, ECIH*

Principal Security Consultant, CEO, Owner

Assistant Professor[1] at Munich University of Applied Sciences

Assistant Professor[2] at Nuremberg Institute of Technology

Assistant Professor[3] at Deggendorf Institute of Technology

SANS Community Instructor° (SANS-Institut: SysAdmin, Audit, Networking and Security)

GIAC Advisory Board Member (Global Information Assurance Certification)

OWASP Leader, Hacking Lab Teacher, Lifetime Member (Open Web Application Security Project)

Former Member of ISSECO (International Secure Software Engineering Council)

ITILv2 Service Manager (Information Technology Infrastructure Library)

[1] „Ethical Hacking“, Department of Computer Science and Mathematics

[2] „Web Application Security“, Faculty of Computer Science

[3] „Offensive Web Application Security“, Faculty Electrical Engineering and Media Technology

° „SEC642 - Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques“

*Glossary:

CISM	Certified Information Security Manager, ISACA
CISSP	Certified Information Systems Security Professional, (ISC)²
GWAPT	GIAC Web Application Penetration Tester, SANS SEC 542
ECIH	EC-Council Certified Incident Handler

1.4. Historisches über Ralf

Mit 11 Jahren fing ich an, meinen Vater um einen C64 (8-Bit *Heimcomputer*) zu bitten.Tag für Tag, Woche für Woche. Zum 13. Geburtstag bekam ich ihn endlich, mit „*Datasette*“ und ausgemusterten S/W-Fernseher. Mit 17, mit *Wählscheibentelefon und Akustikkoppler* „*raste*“ ich damit (300 *Baud*, entspricht etwa 2,75 MB/*Tag*) um die Welt. Ich wurde Mitglied im CCC und nutzt eine selbstgebaute *Bluebox*, um auch schon mal mit einem Satelliten direkt zu „sprechen“ (mit C5), wenn ich *DM 20,- für eine Stunde Hamburg* oder *DM 240,- für eine Stunde USA* für unangemessen hielt. Erzogen von meiner Oma achtete ich dabei sorgsam darauf, nie jemandem auch nur einen Cent echten finanziellen Schaden zu verursachen, sondern nur die „Features“ des Systems (aus) zu nutzen. Ein bisschen später holte ich mir ein Modem mit 2.400 *Baud*, direkt aus den USA und nicht von der Post zugelassen. Mit dem Anklemmen dieses Gerätes an die alte *ADo-Dose* sparte ich mir zwar DM 2.200,- Anschaffungskosten (soviel war der fehlende *Aufkleber des Fernmeldetechnischen Zeugamts* vermutlich wert), riskierte dafür aber nach dem *Fernmeldeanlagengesetz* von 1928 die gleiche Strafe wie für das fahrlässige Auslösen eine *Atomexplosion*, nämlich 5 Jahre.

Passwörter waren generell nicht so gut (oder standen auf einem Zettel), viele Systeme liefen ungehärtet in der Standard-Konfiguration, hatten Gast-Zugänge und massig Fehler. Den 18. feierte ich nicht ganz so ausgelassen wie meine Schulkameraden; ich hatte das Gefühl, zukünftig ein wenig langsamer machen und mein *Risiko-Management* verbessern zu müssen. So war das Ende der 80er, bzw. Anfang der 90er, als man mit „*Cyber“* in der Regel noch „*Cyber Sex“* meinte.

Bei mir hat sich in der Folge einiges geändert: Nach einer *normalen IT-Karriere: Studium - Administrator - Entwickler - Consultant - Projektleiter – Teamleiter*, bekam ich 2008 die Chance, *Information Security* nicht nur am Rande und als Hobby, sondern als bezahlten *Vollzeitjob* zu betreiben! Ernsthaft: Wie toll ist das denn, bitte? Du kannst nicht nur den ganzen Tag hacken, Du bekommst auch noch die geilsten Targets von Banken, Versicherungen, Behörden und DAX-Konzernen auf dem *Silbertablett serviert*, wirst noch mit *Insider-Informationen versorgt* und zum Teil auch direkt unterstützt und bekommst Applaus und Schulterklopfen, wenn das System so richtig die Grätsche macht. Du merkst, dass Du wirklich dabei hilfst, Dinge zu verbessern. Eigene Forschung wurde ermöglicht, und bereits 2009 hatte ich mein erstes *Whitepaper* und hielt meinen ersten „großen“ Vortrag auf einer mehrtägigen Konferenz mit 14.000 Teilnehmern. Dabei war ich nicht völlig undankbar, als *Rookie* nur einen von fünf *Nebensälen* bespaßen zu müssen.

Schnell stand fest, dass diese *alte Liebe* sicher kreativer, holistischer und noch erfolgreicher umsetzbar wäre, wenn man seinen eigenen Kunden nach eigener Vorstellung und natürlich auf

eigene Rechnung betreuen könnte. So habe ich 2010 mit einem Kollegen die *sic[!]sec GmbH* gegründet: „*Kunden-Budget erschöpft, dauert aber länger? Egal, es ist spannend, jetzt wollen wir es wissen! Ehrenamtliche Tätigkeit für die Community? Solange es Spaß macht und allen einen Mehrwert bringt, ganz sicher! Konferenz-Teilnahme oder Wunschzertifikat super teuer? YOLO! Das letzte Hemd hat keine Taschen, Dein Wissen nimmt Dir niemand mehr.“*

Information Security ist *sexy*. Vermutlich hat es deshalb die Politik und Wirtschaft geschafft, diesen schönen Begriff durch *Cyber Security* zu verdrängen. 30 Jahre, nachdem ich meinen C64 bekam, saß ich fast zwei Jahre lang jedes Quartal in Berlin mit etwa 40 anderen weißen alten Männern (und natürlich einigen Damen) zusammen. Wir waren die Expertenkommission „*Informationsaustausch und operative Sicherheitsprozesse*“. Wir durften Kaffee trinken, Kekse knabbern und zusammen mit anderen Expertenkommissionen, von denen ich persönlich und inhaltlich nicht allzu viel mitbekam, an der „*Nationalen Wirtschaftsschutzstrategie 2015*“ mitarbeiten. Die kam dann auch 2016 - ganz pünktlich und feierlich - raus. Vorgestellt von den Präsidenten des *BDI, DIHK, BSI, BKA, BND, Verfassungsschutzes*, usw. Wow! Ein echtes „*Leuchtturmprojekt“*! Oder konkreter:

Man hatte eine Website gebastelt, „*wirtschaftsschutz.info*“. Als Self-Service, für jeden, den es interessiert und der sich die Mühe macht, einen Account zu beantragen und dann vielleicht auch einen bekommt. Ich habe kurz für Sie nachgesehen - diese Seite hat auch *keinen Aufkleber* vom Fernmeldetechnischen Zeugamt (2002 wurde übrigens das Fernmeldeanlagengesetz beerdigt).

Passwörter waren generell nicht so gut (oder standen auf einem Zettel), viele Systeme liefen ungehärtet in der Standard-Konfiguration, hatten Gast-Zugänge und massig Fehler. Dieses Leuchtturmprojekt feierte ich nicht ganz so ausgelassen wie meine Cyberkameraden; ich hatte das Gefühl, zukünftig weniger Zeit verschwenden und mein Pro-Bono-Management verbessern zu müssen.
So war das Mitte der 10er Jahre, als man mit „*Cyber“* fast nur noch „*Cyber Security*“ meinte.

Ich teile gerne, die Welt muss besser und Wissen muss weitergegeben werden. Neben individuellen oder allgemeinen Schulungen und Trainings für Kunden, Awareness-Maßnahmen durch *Social Engineering oder Live Hacking* war ich nicht nur langjährig bei *OWASP* und *SANS* engagiert, ich habe zwischenzeitlich auch Lehrbeauftragungen an drei deutschen Hochschulen angenommen. Mittlerweile darf der ehemalige Rookie gelegentlich auch mal den *großen Saal* bespielen und die *Key Note* halten. Und er hat Spaß daran!

Das Wissen um erfolgversprechende Angriffs-Vektoren nutze ich u.a. für *Digitale Forensik*, falls der

Angreifer doch von der „Gegenseite“ kam und schneller oder besser als die Verteidiger war, aber auch mittendrin, wenn der Angriff gerade noch läuft und die „Cyber-Hütte“ schon lichterloh brennt und ich als *Incident Responder oder Handler* unterstützen kann.

Seit Oktober 2020 bin ich - nachdem ich 10 Jahren als Principal Security Consultant und Geschäftsführer dem Team der sic[!]sec mit Rat und Tat zur Seite stehen und ich meinen persönlichen Frieden mit „cyber" machen durfte - für die „*CYBEReinhardt GmbH*" unterwegs.
Der Name ist Programm. Wie kann ich *Ihnen* konkret weiterhelfen?

Wenn Sie jemanden suchen, der Ihnen Ihre Anwendungen, Systeme oder die Organisation aufbaut und absichert, so bin ich der Falsche für Sie. *Ich bin kein Builder, ich bin ein Breaker*, ich verkaufe auch nichts (außer Lebenszeit).

Ihre Builder sagen Ihnen, dass sie fertig und Sie nun sicher seien. Ihre Defender sagen, sie hätten alles im Griff. Wenn Sie das nicht einfach so glauben, sondern es genauer wissen wollen - dann bin ich Ihr Mann! Wenn Sie es vielleicht zunächst nicht so genau wissen wollten und jetzt ein Problem haben - dann bin ich auch Ihr Mann. Brand bekämpfen, Feuer löschen, Brandursache feststellen, mit Behörden und Versicherungen sprechen mache ich gerne (bitte ergänzen Sie dabei mental „Cyber“ vor jedem einzelnen Substantiv).

Natürlich kann ich Ihnen auch gerne sagen, wie andere bestimmte Probleme gelöst haben, was oft oder ganz Allgemein als „*good practice*“ angesehen wird oder was ich in Ihrem konkreten Fall evtl. tun würde („*best practice*“ ist es übrigens, regelmäßig zu atmen und nicht zu ersticken - alles andere „*best*“ könnte leicht Richtung „*buzzword bingo*“ gehen).
Die konkrete Umsetzung und ggf. „Lösungs“-Auswahl muss aber von Ihren Buildern kommen.

Gerne berate und schule ich Sie und Ihr Team vor oder während der Umsetzung. Geht diese Beratung sehr tief, dann bin ich allerdings als Breaker für Sie *verbrannt*. Betriebsblindheit beim Test, Assessment oder Audit heißt, genau das zu prüfen, was man selbst empfohlen hat. Diesen *Bock zum Gärtner* machen können nur die Big Four oder Überwachungsvereine, die behaupten, *Cyber Security Consultants* und *Breaker* seien bei ihnen *disjunkte Abteilungen*, die nicht miteinander reden würden.

Am Ball bleiben, miteinander reden und sich austauschen ist aber „*Key*“ in Sachen „C*yber*“ :-)
Es ist ein Windrundhennen, bleiben wir einfach dran! Schöne Grüße, Ralf Reinhardt