Evolution Security GmbH

Penetrationstest & IT-Sicherheitsdienstleistungen

Übersicht:

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Mobile: +49170/6923766

Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel, Hessen in Germany
Telefon: +49(0)561-40085396

Email: admin@evolution-sec.com
Email: bkm@evolution-sec.com
Email: service@evolution-sec.com

1. Einleitung

Die Evolution Security GmbH schützt Software, Dienste, Applikationen, Hardware oder Betriebssysteme auf verschiedensten Plattformen und informiert den Hersteller auf sicheren Wegen. Wir bieten unseren Kunden fortschrittliche Penetrationstests, Sicherheitsprüfungen und Schwachstellenanalysen.

Das gezielte Ausnutzen von Sicherheitslücken und Schwachstellen, die Verwertung mit Leistungsprogrammen, Penetrationstests, Audits, Bug Bounty Programme oder das verantwortungsvolle offenlegen von Sicherheitsproblemen ist unser tägliches Geschäft.

2. Evolution Security GmbH - Firma (Über Uns)

Die Evolution Security GmbH bietet Ihre Dienstleistungen erfolgreich internationalen Unternehmen aller Größenördnungen und Sektoren an. Wie viele mittelständische Unternehmen, zählen wir auch über 20 Konzerne zu unserem aktiven Kundenkreis. Da die Zufriedenheit des Kunden für uns oberstes Gebot ist, bieten wir unserem Kunden bei der Durchführung von Sicherheitstests an, persönlich vor Ort zu sein, um so aktive Einblicke in unsere Vorgehensweise und Arbeitsabläufe zu gewähren.

Start, Verwaltung & Gründung

Die Evolution Security GmbH arbeitet im Auftrag führender Technologieinstitute der westlichen Welt. Unsere Firma verfügt über tiefes technisches Wissen im Bereich der IT-Sicherheit, Kreativität und besitzt Zugang zu einem aktiven internationalen Netzwerk für Sicherheitsforscher. Die leitenden Beauftragten tauschen Informationen in verschiedensten Ländern aus, um aus einer neutralen Perspektive als unabhängiges Sicherheitsteam zu agieren. Die unabhängige und nicht-kommerzielle Evolution Security Sicherheitsforschungsarbeitsabteilung kam zum ersten Mal im Dezember 1997/1998 zusammen. Nachdem sich die selbstständige Firma Evolution Security auf dem öffentlichen Markt platziert hatte, änderte der Inhaber durch eine Kapitaleinlage die Rechtsform in 2014 zu einer rechtsgültigen GmbH. Der Geschäftsführer der Evolution Security GmbH und der Vulnerability Lab Initiative ist Benjamin Mejri (Kunz). Er ist bekannt als das Rückgrat der Sicherheitsfirma und ist der leitende Direktor. Unsere Sicherheitsfirma ist offiziell seit 2014 in Deutschland bei der Industrie und Handelskammer in Kassel - Hessen registriert.

Konzepte & Dienste

Die Mythologie unserer Sicherheitsfirma ist verbunden mit einem Konzept, dass auf Vertrauen, Zuverlässigkeit und Ehrlichkeit im Umgang mit Kunden basiert. Lange Ausarbeitung der Partner-schaften, technischen Kenntnisse und Kooperationen sind unser innovativer Schlüssel zum Erfolg.

- Sicherheitslücken, Schwachstellen, Penetrationstests & Audits
- Schutzmaßnahmen, Preventionstechniken & Verschlüsselung
- Sicherheitsnachrichten, Diskussionen & kommentierte Berichte
- Programmierung, Forschung & Sicherheitsmanagement
- Risikoanalysen, Entwicklerbeschreibungen & Sicherheitsvideos
- Vorträge, Workshops, Schulungen & Präsentationen

Philosophy des Penetrationtests & Security Teams

Unser Sicherheitsteam wird einen individuellen Sicherheitstest oder Penetrationstest als Lösung für Ihre Anforderungen im Bereich der IT-Sicherheit mit Ihnen erarbeiten. Unsere Firmenphilosophie ist nicht darauf ausgelegt mit "üblichen" Scanning-Anwendungen oder Skripten zu testen, diese verwenden wir während der Prüfung nur als Ergänzung zu unseren speziellen manuellen Sicherheitsprüfungsverfahren. Unser internationales Sicherheitsteam mit einer langjährigem Fachwissen ist immer bereit für neue Herausforderungen. Wir würden uns freuen Ihre Software, Online Dienste, Anwendungen, Applikationen, Produkte, Automaten oder Infrastruktur auf Schwachstellen und Sicherheitslücken zu überprüfen.

" Our ambition is your security! "

3. Referenzen der Sicherheitsfirma

Die Evolution Security GmbH Unternehmen ist verbunden mit dem Vulnerability Laboratory Team und nimmt ebenfalls an unkommerziellen Sicherheitsprogrammen teil (Responsible Disclosure). Wir nehmen nur an den bekanntesten unkommerziellen Sicherheitsprogrammen teil die sich mit Web-Applikationen oder Software Produkten beschäftigen.

Unsere erfahrenen Experten und Sicherheitsbeauftragten nehmen schon seit 2009 an verschiedenen unkommerziellen Sicherheitsprogrammen von Herstellern wie Microsoft (MSRC), Oracle Corporation, Apple, Adobe, Nokia or AT&T teil. Die nun folgenden Links zeigen offizielle Referenzen als Bestätigung für die Sicherheitsforschung der Evolution Security GmbH zur Aufdeckung von Zero-Day Schwachstellen und Sicherheitslücken.

Reference(s): Public Security Acknowledgments

www.support.apple.com/kb/HT1318

www.paypal.com/webapps/mpp/security-tools/wall-of-fame-honorable-mention

www.adobe.com/support/security/bulletins/securityacknowledgments

www.oracle.com/technetwork/topics/security/securityfixlifecycle-086982

www.developer.att.com/developer/apiDetailPage.jsp

linkedin.com/app/answers/detail/id/37022

www-03.ibm.com/security/secure-engineering/report.html

www.nokia.com/global/security/acknowledgements/

www.us.blackberry.com/business/topics/security/incident-response-team/collaborations

www.pages.ebay.com/securitycenter/ResearchersAcknowledgement

www.technet.microsoft.com/en-us/security/cc308589

www.security.yahoo.com/article.html

www.vodafone.de/unternehmen/soziale-verantwortung/sicher-im-dialog.html

4. Vulnerability Research Laboratory (Program)

Das Vulnerability Lab Team arbeitet hart daran Europa und der Welt eine größere Menge an Informationen im Bezug auf Sicherheitslücken und Schwachstellenreports zugänglich zu machen. Vulnerability Lab kann eine äußerst wertvolle Ressource für Informationen sein, wenn Sie ein Hersteller oder Geschäftskunde sind.

Das Vulnerability Laboratory Core Research Team indentifiziert unabhängig eigene Schwachstellen, Sicherheitslücken oder Fehlkonfigurationen & informiert die Hersteller rechtzeitig sowie professionell auf sicheren Wegen.

Der Prozess der Entwicklung und Freigabe einer Schwachstellen oder eines Advisories wird immer in einer professionellen Art und Weise verfolgt. Sensible Informationen können zensiert werden und jeder Beitrag von Dritten ist nicht erlaubt. Bösartige Datenpakete oder gestohlene Inhalte sind im Labor nicht erlaubt. Weitere Informationen dazu finden Sie im Labor Hilfeseite. Vulnerability-Lab bietet nicht nur Advisories für Software, Applikationen oder Systeme, sondern auch die individuelle Anpassung dieser Advisories für bestimmte Anbieter oder Arten von Schwachstellen. Zusätzlich beinhalten die Berichte wichtige Daten in Form von Ressourcen und Videos von Sicherheitstests.

Wenn es Ihr Ziel ist über neue Sicherheitslücken in der Software, Applikationen & Systemen informiert werden, können gerne mit unseren Kern-Forschern und der Infrastruktur koopieren. Das Sicherheitslabor steht für Wissen in Form von Bildung aus dem Forschungsbereich und ist eine öffentliche Infrastruktur zum melden von Sicherheitslücken oder Schwachstellen. Bitte lesen Sie unser Nachrichten Magazin oder treten Sie dem öffentlichen Vulnerability Laboratory Programm als Forscher bei. Die Vulnerability Lab Programm Initiative sieht sich verpflichtet Sicherheitslücken und Schwachstellen in Software, Service-, System- oder Web-Applikationen" aufzudecken, um diese direkt an den Hersteller zu übermitteln.

Websites/Domains:	www.vulnerability-lab.com or www.vuln-lab.com
Contact Administration:	admin@vulnerability-lab.com
Support Team:	support@vulnerability-lab.com
Research Team:	research@vulnerability-lab.com
Submit Advisories/Vulnerabilities:	submit@vulnerability-lab.com

5. Referenzen des Sicherheitslabors

Die Veröffentlichung eines "Bulletin", ist ein aktuelles Ereignis, dass verhindern soll das es zu keiner Unterbrechung der geplanten sicheren Programmierung kommt oder ein Nachrichtenereignis um über Details zu berichten. Sehr oft kommt es dabei vor das schon berichtete Geschichten aus einem Netzwerk aufbereitet werden für konkrete Erfassung. Die Verwendung ist oft lose orientiert an den bedeutendsten Sicherheitsgeschichten des Augenblicks oder einem speziellen Vorfall der übertragen wird. Es könnte z.B. eine Geschichte mit Hintergrund sein, die einfach von breiten Interesse für die Zuschauer ist und nur direkte Auswirkungen hat.

Das Evolution Security Team arbeitet mit bekannten Herstellern wie z.B. Microsoft, Dell, eFront, Facebook, IBM, Fortinet, FortiGuard, Woltlab, AT&T, Sonicwall, PayPal Inc, Ebay oder Barracuda Networks zusammen um Schwachstellenberichte in unserem Kundenbereich, dem Downloadcenter oder den Monitoringsystemen bereitzustellen. Die nun folgenden "Bulletins" (Schwachstellenberichte) wurden von Herstellern veröffentlicht um zu verhindern, dass die

entsprechenden Sicherheitslücken ausgenutzt werden können.

Link Reference(s):

www.technet.microsoft.com/en-us/security/bulletin/ms13-067
www.esupport.trendmicro.com/solution/en-US/1096805
www.fortiguard.com/advisory/FG-IR-013-001/
www.fortiguard.com/advisory/FG-IR-012-007/
www.fortiguard.com/advisory/forticloud-cross-site-script-persistent-web-vulnerabilities
www.fortiguard.com/advisory/fortimanager-and-fortianalyzer-xss-vulnerability
www.fortiguard.com/advisory/fortimanager-and-fortianalyzer-client-side-xss-vulnerability
www.fortiguard.com/advisory/fortimanager-and-fortianalyzer-persistent-xss-vulnerability
www.fortiguard.com/advisory/fortimanager-and-fortianalyzer-persistent-xss-vulnerability
www.web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5169
www.barracuda.com/support/knowledgebase/501600000013m1P
www.barracuda.com/support/knowledgebase/501600000013lXe
www.barracuda.com/kb?id=501600000013gvr
www.sonicwall.com/us/shared/download/Support_Bulletin_-_Scrutinizer_Vulnerabilities
www.sonicwall.com/us/shared/download/Support_Bulletin_SonicOS_Web_Script_Vulnerability
www.sonicwall.com/us/shared/download/Dell_SonicWALL_SRA_Vulnerability_Service_Bulletin
www.sonicwall.com/us/shared/download/Support_Bulletin_GMS_Analyzer_Vulnerability
www.debian.org/security/2016/dsa-3622
web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6186
web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0956
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2018
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6186
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6767
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3196

6. Angebotene Dienste (Penetrationstests & Details)

Das Evolution Security Team und das Vulnerability Laboratory Research Team kombinieren Dienstleistungen um dem Kunden unterschiedliche Option von Sicherheitstests & Sicherheitsprüfungen anzubieten. Schauen Sie sich gerne unsere einzelnen Dienstleistungen in aufgelisteten Kategorien an.

- Automatisierte Penetrationstests
- Manuelle Penetrationstests

- Whitebox Prüfverfahren
- Blackbox Prüfverfahren

- Mobile & VoIP Systemsicherheit
- Geldautomaten & Zahlungssystem Sicherheit
- Spiel-, Gewinn- & Ticket-Automaten Sicherheit
- Hardware & Embed System Sicherheit

- Präsentationen & Vorträge
- Live Hacking & Veranstaltungen
- IT-Scherheit Workshops

Wenn Sie Fragen oder Anregungen bezüglich unserer Dienstleistungen haben, können Sie sich jeder Zeit an unsere support service teams. Bitte schauen Sie sich unsere Hauptkategorien zum Penetrationstest an um unsere Dienstleistung genau erläutert zu bekommen.

Unsere Kunden sind überwiegend in folgenden Technologiebereichen angesiedelt:

- Banken, Kanzleien, Zahlungsdienstleister und Versicherungen
- Telekommunikations-, Überträger & Web-Dienstleister
- Behörden der Bundesländer und Landesebenen
- Internationale Konzerne & Industrie - Automotive, Chemie, Energie, Wasser & Medien
- Universitäten, Institutionen, Portale & Agenturen

7.1 Manuelle Penetrationstests

Bei der Evolution Security GmbH sind unsere Sicherheitsexperten den Hackern und kriminellen Tätern im Internet immer einen Schritt voraus, durch den täglichen Umgang mit Sicherheitslücken oder Schwachstellen. Unsere Team-Mitglieder sind bereits bekannt für Ihre manuellen Testmethoden und werden von den beliebtesten Anbieter im Internet für die Suche von Zero-Day Schwachstellen oder zur allgemeine Berichterstattung anerkannt. Unsere Referenzen beziehen sich auf frühzeitig manuell aufgedeckte Sicherheitslücken oder Schwachstellen in wichtigen Produkte von Herstellern wie z.B. Sony, Trend Micro, Barracuda Networks, AT&T, Ebay, Paypal Inc, Google, Facebook oder Mozilla.

Bei der manuellen Penetrationstests Prozess wird jede einzelne Anfrage sorgfältig analysiert und überwacht, um sicherzustellen, dass uns keine Problemtiken und Schwachstellen entgehen. Dies kann die Zeitdauer des Projekts während der Testsimulation erhöhen, gleichzeitig sorgt dies aber für eine 100% erfolgreiche Quote im Bezug auf die Ergebnisse mit Fehlalarmen (false/positiv).

Die Art der Tests variieren je nach Umfang der Arbeit des Kunden jedoch unten aufgeführt ist eine allgemeine Liste von Tests, die unser Team während des manuellen Penetrationstests durchführt.

- Authentication
- Authorization
- Sitzungsstatusverwaltung
- Eingabevalidierung
- Web-Datenspeicher
- XML/SOAP Web Dienste
- Web Applikation Management
- Bekannte Sicherheitslücken und Schwachstellen
- Unvalidierte Eingaben
- Defekte oder Fehl konfigurierte Zugriffskontrolle
- Defekte Authentifizierung und Sitzungsverwaltung
- Web Session Schwachstellen und Sicherheitslücken
- Cross Site Scripting (XSS)
- Buffer Overflows
- Script Code Injection Flaws
- SQL Injection Flaws
- Format Strings
- Stack- & Heap- Overflow
- Fehlerhafte Handhabung & Management

- Unsichere Speicherung
- Denial of Service
- Unsicheres Konfigurationsmanagement

7.2 Automated Penetrationtests [ARPT - Automated Rapid Penetration Testing]

In manchen Simulationen kommt aufgrund der spezifischen Anforderungen einer Sitzung von Projektlaufzeiten unser neues ARPT (Automatische Schnelle Penetration Testing) Model zum Einsatz. Während dieses Prozesses werden verschiedene Werkzeuge und Programme verwendet. Diese automatisierten Programme werden von den Fachinformationssicherheitsexperten und Sicherheitstechnikern entwickelt und sind meist Open-Source, öffentlich lizenziert oder vom Vulnerability Lab selbst entwickelt worden.

Da das automatisierte Testen mit Anwendungen zu Fehlalarmen neigt, versuchen unsere Penetrationstester alle Aufzeichnungen doppelt überprüfen, um sicherzustellen, dass alle Sicherheitslücken/Scwahchstellen gültig sowie richtig verarbeitet wurden. Dies verbessert die Qualität der Arbeit welche wir verrichten und hilft uns, unsere Arbeit professionell abzuliefern um die Zufriedenheit des Kunden zu garantieren. Unser Team ist nicht abhängig von spezifischen Werkzeugen, Programmen und Scannern. Die Werkzeuge, die von uns in einem automatisierten Penetrationstest verwendet werden, hängen immer über den Umfang und den Gegebenheiten des Jobs im einzelnen Projekt ab.

Die Art der Tests variieren je nach Umfang der Arbeit, des Kunden. Es folgt eine allgemeine Liste von Sicherheitsproblemen die unser Sicherheitsteam während eines laufenden automatisierten Penetrationstests identifizieren kann.

- Authentication
- Authorization
- Session State Management
- Input Validation
- Web datastores
- XML/SOAP web services
- Web application management
- Known Vulnerabilities
- Unvalidated Input
- Broken Access Control
- Broken Authentication and Session Management
- Web Session Flaws & Vulnerabilities
- Cross Site Scripting (XSS) Flaws
- Classic Buffer Overflows
- Script Code Injection Flaws
- SQL Injection Flaws
- Format Strings
- Stack- & Heap- Overflow
- Improper Error Handling
- Insecure Storage
- Denial of Service
- Insecure Configuration Management

7.3 Whitebox (Whitehat) Penetrationtests

Bei einem externen White(Weiß) Penetrationstest stehen hingegen zum Blackbox Test Informationen, Daten und Quellcodes, der Dienste zur Verfügung. Diese Informationen betreffen z.B. die Versionsnummer einer Software, Dienstauskünfte(SSH, FTP, SMTO, TELNET, IMap ..), Infrastruktur Design, Detail Konzepte oder den Quellcode einer Software/Applikation. Beim Umgang mit Elektronischen Mechanismen könnten Schaltpläne, Platinenkonfigurationen, Mappings oder Schemen dazu beitragen qualitativ hochwertige Resultate zu erzielen.

Bei einem Whitebox Sicherheitstestverfahren kooperiert der Auftraggeber mit dem Dienstleister, um dauerhafte Sicherheitslösungen zu generieren. Zusammenarbeit fordert das aktiv Testverfahren gegen die zu testenden Infrastrukturen des Unternehmens.

Bei einem Whitebox Sicherheitstest wir mit dem jeweiligen Hersteller kooperiert, um mit internem Wissen die besten Sicherheitslösungen zu generieren. Im Team kommen unsere Mitarbeiter einfacher an Lösungen und zuverlässige Ergebnisse um Ihr System oder Ihre Infrastruktur ausführlich sowie dauerhaft zu sichern.

Worin liegen die Vorteile beim Whitebox Sicherheitstestverfahren?

- Erhöhung der Schwachstellen & Erkennungsrate
- Schnelleres Abgleichen und Vorgehen bei Penetration Tests & Simulationen
- Netzwerk Risikoanalysen für Infrastrukturen
- Einberechnung von neuen Angriffsvekoren durch die Entwickleransicht

7.4 Blackbox (Blackhat) Penetrationtests

Alle unsere Angebote im Bereich, der Penetrationstests und Sicherheitsaudit sollten in Kombination mit einem Black und White Feature in Anspruch genommen werden. Diese Features verändern je nach Anwendung, das Angriffsbild und die Dokumentation für das weitere vorgehen bei einem Penetrationstest.

Bei einem externen Black(Schwarz) Penetrationstest stehen keine Daten(Quellcode, Betriebsinformationen & Netzwerkinformation) zur Verfügung. Unser Team muss also über Umwege an Informationen und Daten kommen und diese auch kompetent nutzen um ein qualitatives Resultat zu erzielen. Im diesem Testverfahren arbeiten unsere Mitarbeiter aus der Perspektive eines kriminell denkenden Computer Hackers, Cyber Betrügers, Online Saboteurs oder destructiven Crackers.

Worin liegen die Vorteile beim Blackbox Sicherheitstestverfahren?

- Reale Angriffsbedingungen
- Vielseitige Einsichten & Dokumentation
- Nicht offenlegung ihrer Projekte oder Source-Codes

7.5 Web Applikation Sicherheit

Das Evolution Security GmbH Sicherheitsteam hat sich auf das identifizieren von Sicherheitslücken oder Schwachstellen in Web-Applikationen und skriptbasierten Anwendungen spezialisiert. Unsere Sicherheitsfirma ist dafür bekannt, webbasierte Sicherheitslücken und Schwachstellen in Applikationen oder Diensten zu identifizieren, zu melden oder erfolgreich zu schließen.

Die Evolution Security GmbH arbeitet fest mit den unterschiedlichen Herstellern und Unternehmen aller Branchen zusammen um zu gewährleisten, dass Sicherheitslücken in Web-Applikationen möglichst schnell identifiziert, analysiert und erfolgreich geschlossen werden können.

Die Forscher und Penetrationstester der Evolution Security GmbH haben bereits zero-day Sicherheitslücken in den unterschiedlichsten Web-Applikationen identifiziert und geschlossen. Unter anderem haben wir während unserer Tests neue Sicherheitslücken an Organisationen wie z.B. die Nato, das Weiße Haus, der IAEA, der NSA, Die Bundeswehr, der FAA, die EU Comission, der Nasa und dem Chinesischem Ministerium für Commerce weitergeleitet, um kritische Infrastrukturen dauerhaft zu schützen.

Unser Sicherheitsteam prüft Web-Applikationen auf den folgenden Ebenen der Kommunikation:

- Datenbankabfragen und Anbindungen (MySQL, MSSQL, PostgreSQL ...)
- Clientseitige Kommunikation - Serverseitige Kommunikation
- Applikationsseitige Kommunikation
- Eingaben & Ausgabe Mechanismen

Unser Advanced Persistent Threat Team identifiziert & analysiert folgende Sicherheitslücken:

- Clientseitige Sicherheitslücken - Cross Site Scripting, Cross Site Request Forgery, Redirects, Clickjacking, SSRF, ID Hijacking ...
- Serverseitige Sicheheitslücken - Remote Code Executions, Insecure DirectObject References, Remote / Local File Inclusion, SQL Injections, Directory Traversals ...

Penetrationstest werden nach folgendem Schema durchgeführt:

- Reconnaissance
- Enumeration
- Exploitation
- Dokumentation

Bitte kontaktieren Sie uns direkt bei Anfragen, Angeboten oder Aufträgen im Bereich der "Web-Applikation" & "Web-Appliance" Sicherheit.

7.6 Netzwerk Sicherheit

Infrastrukturen mit informationstechnologischen Hintergrund unterliegen einer hohen Dynamik der Geschäftsprozesse und Unternehmensanforderungen durch den fortlaufenden Wandel der Zeit. Weiterentwicklungen wie die Virtualisierung von Server Systemen oder der Umzug in die Cloud erfordern eine kontinuierliche Optimierung der Netzwerksicherheitskomponenten und der Infrastruktur, an die aktuellen Anforderungen des digitalen Zeitalters. Netzwerksicherheit ist ein Prozess der in den Bereich sichere Infrastruktur einzuordnen ist. Dieser Prozess muss dauerhaft stattfinden, um so permanente Problematiken oder neue sowie bekannte Schwachstellen schnell zu erkennen.

Die Evolution Security GmbH begleitet, erstellt, verteidigt und betreut Sie auf diesem Weg im Bereich der IT-Sicherheit. Wir erstellen Konzepte für sichere Netzwerke, analysieren Risiken, bewerten Sicherheitsmechanismen & identifizieren bekannte oder unbekannte Schwachstellen. Unser Team aus Experten kann flexibel vor der Erstellung eines Netzwerks eingebunden werden, natürlich helfen wir aber auch gerne bei schon aufgebauten produktiven Netzwerken. Wir beraten unsere Kunden auf einer zuverlässigen und sicheren Ebene und berücksichtigen dabei alle möglichen sicherheits-relevanten Problematiken.

Netzwerk - Schnittstellen & Komponenten

Netzübergänge wie z.B. die Anbindung an das öffentliche Internet oder ethernet Netzwerk-schnittstellen zwischen unterschiedlichen Bereichen Ihres Unternehmens müssen kontrolliert, geprüft und reglementiert werden, um Dienste und Daten vor unberechtigten Zugriffen zu schützen und die Netzwerksicherheit dauerhaft zu gewährleisten. Dies ist die Aufgabe von Firewalls, Filter Mechanismen und Intrusion Prevention Systemen. Die Evolution Security GmbH entwickelt für Ihr Unternehmen maßgeschneiderte individuelle Lösungen zur aktiven Gewährleistung der Netzwerksicherheit.

Server Systeme & Virtualisierung

Die Einrichtung von Server-Systemen durch Virtualisierung erfordert ständig neue Schutz-maßnahmen zur Gewährleistung der allgemeinen Netzwerksicherheit. Kommunikations-schnittstellen, die früher durch Firewalls gesichert waren, werden zunehmend über den internen Bereich an die Virtualisierungs-Hardware ausgelagert. Bestehende Netzwerksicherheits-Lösungen können nicht oder nur unzureichend den notwendigen Schutz bieten.

Die Evolution Security GmbH unterstützt Sie bei der Angleichung und Anpassung von schon bestehenden Sicherheits-konzepten, um den technischen Herausforderungen der Neuzeit permanent gewachsen zu sein. Bitte kontaktieren Sie uns direkt für Anfragen, Beauftragungen oder Analysen im Bereich der "Netzwerk Sicherheit".

7.7 Mobile & VoIP Penetrationtests

Smartphones sind überall, die Mobilfunkindustrie explodierte in 2010 auf 2013, weil ein endloser Bedarf an Smart Technologie Telefonen von Apple, Microsoft, Nokia, Samsung mit verschiedensten Betriebssystemen wie z.B. Android, iOS or Windows 8 besteht. Die mobile Sicherheit und die Sicherheit von Mobiltelefonen hat in den letzten Jahren im Mobile-Computing-Bereich rasand zunehmend an Bedeutung gewonnen.

Es ist heutzutage von besonderer Bedeutung, dass man sich dauerhaft auf die Sicherheit der persönlichen Informationen bezieht weil Smartphones oder mobilen Geräte persönliche Informationen speichern.

- Mobile Software
- Firmware
- Betriebssystem
- Mobile Web Applikationen
- Hardware
- Schnittstellen

Die Industrie kam in den letzten Jahren mit dem Bedürfnis nach mehr Sicherheit im Mobilfunk oder VoIP-Sektor. Das Ergebnis dazu war, dass unsere Firma die lokale Infrastruktur aufgerüstet hat, um dauerhaft Berichte über Anfälligkeit in Mobilfunksystemen für unsere Kunden oder Partner bereitzustellen. I

m Jahr 2013 entdeckte unsere Sicherheitsfirma z.B. 117 Sicherheitslücken in mobile Anwendungen, 15 Anfälligkeiten von mobiler Firmware, 3 Betriebssystemschwächen & 2 Hardware-Fehler auf. We do operate in the following categories of the mobile pentest business. Wir bieten Dienstleistungen in the folgenden Bereichen der Mobilen Sicherheit an.

- Secure Boot-Firmware-Komponenten
- Ausführung von beliebigem Code mit Kernel-Rechten
- Unberechtigter Zugriff auf Cloud- und Mobile Account-Kontodaten auf mobilen Servern
- Zugriff von einem Sandbox-Prozess auf Benutzerdaten außerhalb der Sandbox
- Fehler oder Sicherheitslücken in Schutzmechanismen
- Extraktion von vertraulichem Material, dass durch Mechanismen wie z.B. den sicheren Enclave-Prozessor geschützt ist
- Kritische Fehler oder Schwachstellen in Zugriffsrechten und Privilegien

Mobile Security Feed - Vulnerability Laboratory

http://www.vulnerability-lab.com/show.php?cat=mobile
http://www.vulnerability-lab.com/search.php?search=phone&submit=Search
http://www.vulnerability-lab.com/search.php?search=apple&submit=Search
http://www.vulnerability-lab.com/search.php?search=ios&submit=Search

Mobile Vulnerability Assessment & Reverse Engeneering

Unsere Firma kann Reverse-Engineering auf jedem App oder gegen jede Firmware unabhängig von Architektur anwwenden. Das Produkt dieser Arbeit ist eine Zuschreibung der Apps-Funktionalitäten, der Inhalte, und wenn eine Bedrohung und / oder angefordert Bedrohung vorliegt bei mobilen Anwendungen, Betriebssystemen, Firmware oder Diensten.

Unser hausinternes Wissen wird von den Mitarbeitern angewendet um den doppelten Zweck der Sicherheitsprüfung unter Verwendung modernster Modelle oder Programme zu gewährleisten. Die Evolution Security GmbH & das Vulnerability-Lab Projekt kooperieren mit tiefen Wissen parallel auf einer Linie für Audits und Sicherheitsprüfungen zu bilden. Dieses Verhalten fungiert als Garantie für die Entwickler eines Projekts.

7.8 Hardware & Embed Systeme - Audits & Penetrationtests

In diesem Bereich bieten wir unterschiedliche Hardwaresicherheits Dienste an. Unsere Hadware- und Sicherheitstests beinhalten detailierte Audits, unabhängige Hackmethoden und individuelle Reverse Engeneering Analysen. Wir sind ebenfalls in der Lage Misskonfigurationen und Hardwarefehler durch Hersteller aufzudecken. Ebenfalls bieten wir Firmenbesuche an, bei denen wir Beispielsweise Router, Kontrolleinheiten, Smartphones, Drucker, Security Appliances oder jegliche Hardware Platinen auf ihre Sicherheit testen.

Unsere qualifizierten Sicherheitstechniker entwickeln und ändern auf kreativem Wege technologisches Zubehör (Hardware) um die Arbeitsprozesse dauerhaft abzurunden. Unser Team beschäftigt sich hauptsächlich mit Hardwarespezifischen Geräten die Computer enthalten und Computern selbst. Die Modifizierung oder Manipulation von analog elektronischen Geräten und mechanischen/elektrischen Zubehör ist unser Geschäft.

Mit unabhängiger Forschung, stillem Vertrauen und exzellenten Reverse Engineering Analysen, kommen wir dem Bedarf des Kunden nach. Unter anderem verfügen unsere Mitarbeiter über Kenntnisse um unsichere Platinenschaltungen, elektronischen Gerätemanipulationen, Hardware Fehlkonfigurationen, Hintertüren und andere unbekannte hwardware-spezifische Geheimnisse zu identifizieren.

Embedded Systeme & Geräte mit verbundener Hardware

Unser Unternehmen arbeitet nicht nur am Schutz von Hardware-Komponenten eines spezifischen Systems, sondern auch an der Sicherung von eingebetteten Systemen die mit Schnittstellen über die Hardware verbunden sind. Im Jahr 2013 entdeckte ein Sicherheitsforscher des Evolution Security Teams eine kritische Firmware Schwachstelle im eingebetteten System der Sony Playstation. Besonders Schwachstellen wie die anerkannte Playstation Sicherheitslücke bei Sicherheitsprüfungen, Audits oder PenTests sind unsere Fachgebiet. Eingebettete Systeme für Geräte wie z.B. die xbox, ps3 und wii erfordern meist ein hohes Maß an innovativen und kreativen Konzepten, um erfolgreich Sicherheitsanfälligkeiten getestet zu werden. Unsere Firma ist in der Lage, innovative und kreative Sicherheitstests von Experten mit fortgeschrittenen Kenntnissen im Themenbereich durchführen zu lassen, um Gerätesicherheit dauerhaft zu gewährleisten.

Unsere Kunden und Klienten ... ?!

Casinos, Spielbanken, Trinkwasser Hersteller, Spiele Konsolen mit Embedded Systemen, Banken (ATMs), Automotive Industry (Embedded Geo oder Navigtationssysteme), Regierungen (Bezahlssysteme), Militärs (ICS), Institutionen wie Strafvollzug (SCADA, ICS & SPS), Krankenhäuser (ICS), Sicherheitsagenturen und Firmen oder Hersteller aus dem Informationstechnologie Bereich. Gerne können Sie uns kontaktieren.

7.9 Automated Teller Machines (Geldautomaten & Ticketautomaten)

Im letzten Jahr haben wir eine neue Sektion in unser öffentliches Portofolio aufgenommen "Automated Teller Machines / Automatensicherheit".

Unser Team verfügt über langjährige Erfahrung in der Cyber Sicherheitsbereich, vor allem wenn es um Geldautomaten von Herstellern wie Wincor Nixdorf, NCR. Keba, Hitachi, Olivetti, Diebold oder GRG geht.

Unser Know-how besteht darin versteckt Hintertüren, zero-day-Schwachstellen, Sicherheitslücken in Diensten und Anwendungsprobleme zu analysieren um Fehler im Design, der Netzwerk-Infrastruktur, dem Ethernet, der Firmware oder Hardware aufzudecken.

Natürlich prüft unser Team auch privilegien, domain controller, system accounts, boot priorities, bios setups und verschiedene andere im Produktivsystem integrierte Module oder eingebettete Funktionen.

In der nun folgenden Auflistung benennen wir die verschiedenen Testbereiche, die bei einem Penetrationstest gegen Geldautomaten wichtig sind ...

- Bios Sicherheit (Boot Prioritäten, Default Konfiguration & Passwort Sicherheit)
- Examination by usage of compromising boot medias
- Sicherheitsprüfung des IDS, Anti-Virus, Firewall & Schutzmechanismen
- Examination of key, hdd or information encryption
- Angriffe über das Netzwerk und Schnittstellen (Produktive Systeme und Testumgebungen)
- Sicherheitsprüfung der Software vom Betriebssystem (Client & Server)
- Sicherheitsprüfung von verbundenen Web-Applikationen
- Sicherheitsprüfung von Management oder Dienst Konsolen (Terminal & Konsole)
- Sicherheitsprüfung von Schnittstellen (Gui, Control Panel & UI)
- Sicherheitsprüfung des Betriebssystemkerns
- System Passwort Prüfungen - Effizienz & Schwäche (BIOS, System, Network & Schlüssel)
- Sicherheitsprüfung und Absicherung der Ein-/Auszahlungsmodule (Dispenser)
- Konfigurationsprüfung der Hardware zur Identifikation einzigartiger oder statischer Hintertüren (Generisch, Geheime Interactionen/tricks oder Funktionale Kombinationen)
- Untersuchung & Prüfung auf Anfälligkeiten der Kassettenkonfiguration
- Scannen nach bekannten Schwachstellen und Sicherheitsbedrohungen
- Sicherheitsprüfung des Fraud Correlation Systemen und statischen Sicherheitsmechanismen
- Special case scenarios (Reproduktion & Test von existierenden Sicherheitslücken)
- Identifizierung von logischen Fehler in Funktionen (Manuelle Interaktion für Manipulation)

Wir bieten unsere Diensteleistung für die Kunden oder Unternehmenan an, Dienstleister von Banken, Zulieferer oder Hersteller von Geldautomaten. Gerne können Sie uns über unsere Internetseite direkt Kontakt mit uns aufnehmen, um ein Treffen zur Vorschau unserer Expertise oder Dienstleistung einzusehen. Unser Sicherheitsteam arbeitet seit Jahren mit verschiedenen Banken oder Dienstleistern zusammen.

Wir bilden zusammen ein starkes sowie vertrauenswürdiges Kommunikationsnetzwerk "Made in Deutschland" zum melden und aufzeichnen von Sicherheitsproblemen oder Schwachstellen.

7.10 Spiel-, Gewinn- & Ticketautomaten Sicherheit

Unser Sicherheitsteam befasst sich nicht nur mit Geldautomaten, sehr gerne prüfen wir auch Ihre anderen Produktserien, wie Druck-, Ticket- oder Spielautomaten und Interaktionsterminals jeglicher Art. Wir testen Geräte auf Hintertüren, prüfen auf Sicherheitslücken in der Anbindung, testen auf Schwachstellen in Schnittstellen und Firmware oder ermitteln Anfälligkeiten der produktiven Infrastruktur. Wir bekämpfen mit unseren Methoden aktiv kriminelle Banden oder Einzeltäter aus

dem Inland und Ausland, die täglich auf Beutezug gehen.

Wir kommen vor Ort zum Einsatz und prüfen die entsprechenden Serien manuell oder automatisiert, um Ihnen ein höheres Maß an Sicherheit zu gewährleisten. Gerne testen unsere Experten in Ihren Hallen auch Geräte vor dem ersten Einsatz, um sicherheitsrelevante Problematiken frühzeitig zu identifizieren.Grundsätzlich bieten wir in diesem Bereich auf Basis des Vertrauens keine Blackbox Sicherheitstests an, damit wir gemeinsam unter den Augen des Kunden, zuverlässige Lösungen erarbeiten können.

Unsere Firma hilft betroffenen Betrieben durch eigene Präventionsmaßnahmen ein besseres Verständnis zu entwickeln. Wir bieten Schulungen und Präsentationen zum Thema an.

Unsere Sicherheitstechniker können im Rahmen der Dienstleistung folgende Problematiken identifizieren und behandeln.

- Sicherheitslücken (Interface, System & Software)
- Schwachstellen & Fehler (Hardware)
- Sicherheitsprüfung der Anbindung (Netzwerk & Kommunikation)
- Hintertüren (Geheime Kombinationen, System, Software & Hardware)
- Reverse Engineering (Hardware, System & Software)

Zu unseren Kunden der Industriehersteller, die wir bei Dienstleistern auf Sicherheitanfälligkeiten prüfen, gehören namhafte Hersteller wie z.B.

- Gauselmann
- NovoMatic (Novo Line Series)
- NSM Löwen Entertainment
- Bally Wulff

Die folgende Liste zeigt diverse Hersteller, die ihre Ticketautomaten über uns haben prüfen lassen:

- Toyo Network Systems & Integration
- BSC-Europe
- Atron Electronic GmbH
- Elgeba Gerätebau GmbH
- Höft & Wessel AG
- ICA Traffic GmbH
- Scheidt & Bachmann
- Krauth Technologie

Bei weiteren Fragen oder falls Sie mehre Informationen benötigen, kontaktieren Sie uns telefonisch oder über das Kontaktformular.

8. Government Program (Austausch & Kooperation)

Das Sicherheitsteam der Evolution Security GmbH kooperiert im Rahmen eines internen Projekts mit Universitäten, Regierungsakademien und militärischen Institutionen. Wir bieten die Dienstleistung des Projekts nur für Schwachstellenforschung, Verwundbarkeitsanalysen, Schulungen, Weiterbildungen oder Workshops an. Unser neues Projekt wurde ins Leben gerufen, um sensible Informationen von Internetseiten, Online Diensten, Applikationen, Software, Computersystemen oder Hardware zu schützen. Unser Team ist eine vertrauenswürdige Ressource bei Kooperationen verschiedensten Regierungen.

Unser offizieller Dienst für Regierung, Militär, Institutionen & Universitäten?
Das Sicherheitsteam unserer Firma stellt drei verschiedene Dienstleistungen im Regierungsprojekt für Universitäten, das Militär oder Regierungsorganisationen bereit. Die Kategorie, die von unserer Firma als erstes angeboten wird, ist das "Dienste Infrastruktur" Sicherheitsprogramm. Diese spezielle Dienstleistung ist nur für staatlichen Instituten oder offiziellen Organisationen und wirkt sich direkt auf die Prüfung und Härtung der systemspezifischen Dienste aus.

Die zweite Dienstleistung findet im selben Bereich statt, fokusiert sich aber ausschließlich auf das erfassen von Sicherheitslücken oder Schwachstellen in Software Produktserien. Meistens sind diese auch in der öffentlichen APL (Approved Products List) der entsprechenden Regierung aufgelistet. Die Software-Infrastruktur-Sicherheitsprogramm ermöglicht es dem Militär, den Behörden und Sicherheitsagenturen über zero-day Software Sicherheitslücken in Produkten von investigativem Interesse informiert zu werden. Die zweite Dienstleistung im Programm ist auch für die Weiterleitung von Software Sicherheitslücken bei zentralen Prüfungen, Zertifizierungen und Audits verfügbar.

Die dritte innovative Dienstleistung unserer Regierungsdienstes steht für die Sicherheit von "Web-Applikationen" zur Verfügung. Das Web-Applikations-Infrastruktur-Programm für die Sicherheit wirkt sich sicherheitstechnisch direkt auf die genutzten Web-Applikationen, Online Dienste oder Internetseiten aus. Wir härten Applikationen, testen Dienste, protokollieren Schwachstellen und informieren zur Prävention für Regierungstellen oder regierungsnahe Organisationen.

Wie kann ich am neuen Regierungssicherheitsprogramm teilnehmen?
Um an unserem Regierungsprogramm teilzunehmen müssen Sie lediglich eine der 3 Kategorien nach Ihren Bedürfnissen auswählen (Dienste-, Software-, Applikation -Infrastruktur Sicherheitsprogramm) um uns zu kontaktieren. Leider müssen wir vorab darüber informieren das es einige Sicherheitsbestimmungen in der neuen Regierung Präventionsprogramm gibt.

- Es dürfen keine sanktionierten Länder an unserem Programm teilnehmen (Syria, Sudan, Lebanon, Lybia, Afghanistan, Palestina, Iraq, North Korea & Co.)

- Wir erlauben keiner Regierung die Teilnahme an unserem Programm, wenn die Informationen für offensive Operationen genutzt werden, destructive Hintergründe aufweisen oder kriminelle Handlungen unterstützt.
- Keine Firmen ohne Regierungshintergrund oder nicht verifizierbare Regierungsfirmen

Unser Firma tauscht keine privaten Nutzer Kontakte, Partnerverträge, Kontaktadressen oder andere sensible Firmeninformationen mit Regierungen aus. Wir achten mit einem wachsamen Auge darauf, nicht bei offensive Operationen, illegalen forensischen Angriffen oder Infiltrationen mitzuwirken.

8.1 SCADA & ICS Infrastrukturen

Das SCADA and ICS Sicherheitsprogramm steht für größere Firmen aus der privaten und öffentlichen Industry zur Verfügung. Wir veröffentlichen und teilen in diesem Programm Informationen und Ressourcen an Partner, um ausführliche Resultate bei SCADE/ICS Sicherheitsprüfungen zu erzielen.
Der Austausch über das Programm orientiert sich an den verfügbaren Budgets der einzelnen teilnehmenden Unternehmen. Wir bieten unseren öffentlichen Partners, Kunden und bekannten Klienten alle Informationen die Sie benötigen um Ihre SCADA oder ICS Infrastrukturgestützten Produktivsysteme dauerhaft abzusichern. Unsere Experten des Sicherheitsteams sind zeritfiziert und trainiert im Umgang mit SCADA oder ICS.

Die Kunden des SCADA & ICS Security Programm kommen aus folgenden Bereichen ... Wasserverarbeitung, Programmentwicklung, Verkehrsmanagement, Kontrollzentren/Überwachungzentralen, Mobilfunkindustry, Nahrungsindustry oder Stromversorgung. Bitte nehmen Sie an unserem Programm teil um dauerhaft zuverlässige informationen über Schwachstellen und Sicherheitslücken in industriellen Kontrollsystemen sowie SCADA Anlagen.

In unserem SCADA & ICS Sicherheitsprogram arbeitet die Evolution Security GmbH aus Sicherheitsgründen nur mit verifizierten und zuverlässigen Klienten, Kunden oder Partnern zusammen.

SCADA (Supervisory Control And Data Acquisition) ... ?!

Ist eine Art von Industrie-Kontrollsystem (IKS). Industrielle Steuerungssysteme sind computergesteuerte Systeme, die Überwachung von industriellen Prozessen steuert, die in der physischen Welt existieren. Diese Prozesse umfassen industrielle, Infrastruktur und einrichtungsbezogene Prozesse, wie in der folgenden Auflistung beschrieben:

- Industrielle Prozesse umfassen die der Herstellung, Produktion, Energieerzeugung und Veredelung oder kann in kontinuierlichen, Chargen-, sich wiederholende oder diskrete Modi laufen

- Infrastrukturprozesse können öffentlich oder privat sein und umfassen Wasseraufbereitung und -verteilung, Abwassersammlung und -behandlung, Öl- und Gaspipelines, elektrische Energieübertragung und -verteilung, Windparks, Zivilschutz Sirene Systeme und große Kommunikationssysteme

- Facility-Prozesse treten sowohl in öffentlichen Einrichtungen als auch private, einschließlich Gebäuden, Flughäfen, Schiffe und Raumstationen. Sie überwachen und steuern, Heizungs-, Lüftungs- und Klimaanlagen (HVAC), den Zugriff und den Energieverbrauch

8.2 Dienste Infrastrukturen Sicherheit

Unser Sicherheitsteam kooperiert mit militärischen Institutionen, Regierungsfirmen mit Informationstechnologie Hintergrund und internationalen Sicherheitsagenturen. Wir übermitteln

Sicherheitslücken an Bedrohungssysteme, Schwachstellen Aufzeichnungssysteme für Appliances oder Applikationen und natürlich an verifizierte Datenzentren.

Zero-Day Vulnerabilities - Geräte, Sicherheitszentren & Überwachungssysteme
Das Sicherheitsteam der Evolution Security GmbH stellt mit dem "Government Laboratory - Cyber Security Program" eine überaus wirtschaftliche Infrastruktur bereit, die täglich neue Informationen über eingehende Sicherheitslücken oder Schwachstellen bereitstellt. Der Dienst stellt Sicherheitslückenberichte für Sicherheitsappliances, Web-Applikationen, Software oder Online Dienste für verbundene und öffentliche Datenbanken zur Verfügung. Teil unseres Initative ist es ebenfalls die Regierungen oder Institutionen rechtzeitig über kritische Schwachstellen zu informieren, um den Dienst oder die Präsenz unabhängig zu schützen.

Einige Kategorien unserer "Dienst Infrastruktur" der Austausch Partnerschaft finden Sie hier ...

- Schwachstellen und Sicherheitslücken Aufzeichnung oder Überwachung
- Erinnerungssysteme für Schwachstellen Tasks
- National Schwachstellen Datenbanken
- IDS/IPS Schwachstellen Auflistung (DBMS)
- Security Appliance Scwhachstellen Dienste
- Alamierung bei Schwachstellen and Notfall Online Dienste
-

NIST, DHS, SCIP, VCW, CNNVD & Co. - Schwachstellen und Sicherheitslücken (Dienste)

The besten Forscher unserer Firma sind mittlerweile überall auf der Welt in verschiedensten Aufzeichnungs- und Alarmsystemen archiviert worden. Unsere Arbeit wurde von den folgenden öffentlichen Regierungstellen und vertrauenswürdigen Datenbanken anerkannt ... DHS, NIST, MIT, VCW, CNNVD or SCIP. Durch dauerhafte Zuverlässigkeit und Ehrlichkeit beim berichten, können wir auf die original Links der entsprechenden Internetseiten verweisen.

Bitte schauen Sie sich die angehängten Bilder unter dem Artikel an um unsere Referenzen einzusehen. Kontaktieren Sie uns für den Beginn zum Austausch von Informationen über zero-day Sicherheitslücken in Diensten.

8.3 Software Infrastruktur Sicherheit

Unser Team kooperiert mit militärischen Institutionen, Regierungs Sicherheitsfirmen und Sicherheitsagenturen. Wir stellen für Software & Produkte eigens entwickelte zero-day Sicherheitslücken bereit, um sensible Regierungsinfrasturkturen zu schützen oder um Cyber-Attacken zu abzuwehren.

Zero-Day Vulnerabilities - Software & Produkt Serien

Das Evolution Security Team stellt mit dem Vulnerability Laboratory eine exzellente Infrastruktur für eine tägliche und wöchentliche Informationsquelle bezüglich Sicherheitslücken. Wir stellen 0day Sicherheitslücken in Regierungs Software Clients bereit, um wichtige interne und externe Software Infrastukturen zu schützen.

Dieser Service wurde erschaffen, um einen Austausch von Sicherheitslücken mit Regierungsstellen zu vereinfachen. Dabei liegt der Fokus des Services, Software Produkte und Serien welche von Regierungsstellen genutzt werden, zu untersuchen und zu schützen. Ebenfalls prüfen wir regelmässig die jährliche "US APL" (Approved Product List), eine von der US-Regierung

zertifizierte Produktliste zur Militär und Regierungs nutzung.

Kunden unseres "Software Infrastruktur" Partner Austausch Programmes

- Militär
- Regierungsorganisationen
- Sicherheitsagenturen
- Institutionen

Software Security Program - Vulnerability Exchange (Dienst)

Die Topresearcher unseres Labors, sind Weltweit auf verschiedenen Schutz- und Sicherheitszentren durch Bekanntmachung von Sicherheitslücken gelistet. Falls sie Fragen zu unserem Service haben, kontaktieren Sie uns.

8.4 Web Application Infrastruktur Sicherheit

Unser Team kooperiert mit militärischen Institutionen, Regierungs Sicherheitsfirmen und Geheimdiensten. Wir stellen Software & Produkte(-Link) 0day-Sicherheitslücken bereit, um sensitive Regierungsinfrasturkturen zu schützen. (We are well known for detecting 0day web vulnerabilities in all kind of online service infrastructures like banks, airports, government websites and service or military networks???). Researcher des Evolution Security Teams haben bereits 0day Sicherheitslücken in unterschiedlichen Web-Applikationen wie die Nato, das weiße Haus, der IAEA, der NSA, der Nasa und dem Chinesischem Ministerium für Commerce? gefunden.

Zero-Day Web Applikation Sicherheitslücken - Online & Web Dienste

Das Evolution Security GmbH Unternehmen und Forschungsteam verfügt über ein eigenes Web-Applikation Infrastruktur Sicherheitsprogramm für Regierungen und Militärs.
Wir bieten unsere Dienstleistung in erster Linie nur an verifizierte und vertrauenswürdige Klienten an um Audits, Penetrationstests oder andere Sicherheitsprüfungen vorzunehmen.
Unsere zweite Dienstleistung aus diesem Bereich ist unser Schwachstellen Meldeprogramm, dass Sicherheitslücken aktiv aufzeichnet um kritische Regierungsinfrastrukturen schnell gegen Cyberangriffe abzusichern.

Kunden unseres "Web Application Infrastructure" Exchange Partnership Programm

- Regierungs Banking & Transaktions Applikationen
- Government Service IPS Application
- Regierungs, Armee und Militär Website Applikationen
- Militär Web Applikation & Control Management Interfaces
- Regierungs Online Dienste & UI (Nutzeroberfläche)
- Web Filter-, Secure Engine und Protection Web Applications

Application Security Program - Vulnerability Exchange (Web Applications)
Wir sind in der Lage, alle möglichen Arten von Sicherheitslücken aufzudecken. Unter anderem Session basierte Probleme, Encodierungsfehler, Cross-Site Probleme, Sql-Injections, Authorisierungs bypass Sicherheitslücken und viele weitere. Falls sie Fragen zu unserem Diensten

haben, kontaktieren Sie uns. Weitere Informationen mit mehreren Details Für Regierungsinstitutionen, Programme oder dem Militärangebot finden Sie hier. Folgende Bilder zeigen veröffentlichte Sicherheitslücken in wichtigen Software Produkten.

9. Penetrationstest (4 Phases - Simulation)

Penetrationstest ist der fachsprachliche Ausdruck für einen umfassenden Sicherheitstest einzelner Rechner oder Netzwerke jeglicher Größe. Unter einem Penetrationstest versteht die Sicherheitsfachperson in der Informationstechnik die Prüfung der Sicherheit möglichst aller Systembestandteile und Anwendungen eines Netzwerks- oder Softwaresystems mit Mitteln und Methoden, die ein Angreifer (Hacker) anwenden würde, um unautorisiert in das System einzudringen (Penetration). Der Penetrationstest ermittelt somit die Empfindlichkeit des zu testenden Systems gegen derartige Angriffe. Wesentlicher Teil eines Penetrationtests sind Werkzeuge, die dabei helfen, möglichst alle Angriffsmuster nachzubilden, die sich aus den zahlreichen bekannten Angriffsmethoden herausbilden.

Penetrationstests sind aus folgenden Gründen nützlich für Unternehmen und Firmen:

- Die Bestimmung der Durchführbarkeit eines bestimmten Satzes von Angriffsvektoren
- Die Identifizierung von Sicherheitslücken mit hohem Risiko, die aus einer Kombination von geringerem risikobehafteten Schwachstellen in einer bestimmten Reihenfolge zur ausnutzung führen
- Identifizierung von Schwachstellen, die schwierig oder garnicht erkannt werden, bei automatisierten Netzwerktests oder beim Einsatz von Anwendungen zum Scannen nach Sicherheitslücken
- Die Beurteilung der Größenordnung von möglichen geschäftlichen und betrieblichen Auswirkungen von erfolgreich simulierten Angriffen
- Testen der eigenen Fähigkeiten bei der Verteidigung von Netzen im Umgang mit der Erkennung und Reaktion bei Angriffen
- Der Nachweis einer erhöhter Investitionen durch Sicherheitstests oder zur Investition bei Unterstützung durch Technologie
- Zertifizierungen durch jährliche Sicherheitsprüfungen oder Penetrationstests

Bitte schauen Sie sich unsere Hauptkategorien zum Penetrationstest an um die einzelnen Unterbereiche erläutert zu bekommen.

- Reconnaissance
- Enumeration
- Exploitation
- Dokumentation

Penetrationstests sind meistens Bestandteil eines vollständigen Sicherheitsaudits einer Infrastruktur. Darunter fallen z.B. auch die Payment Card Industry Data Security Standards (PCI DSS) und der allgemeine Sicherheits- und Prüfungsstandard, sowohl wie die jährlichen und laufenden Penetrationstest-Statistiken (nach Systemänderungen).

9.1 Reconnaissance (Information Gaterhing)

Technische Informationen könnten zum Beispiel sensible Daten in Web-Server-Hosting / Informationen, IPS / IP-Bereiche, das Wissen über Hardware/Software Versionen, Module, Modelle, Informationen über die internen oder externen Netzwerkinfrastruktur eines Unternehmens.

Nicht-technische Informationsbeschaffung

Nicht-technische Informationen können zum Beispiel unternehmensinterne Strukturen (Büro), die Lage (Firma), das Gebiet (Land), Mitarbeiter, interne Telefonnummern, E-Mail-Adressen zu sozialen Unternehmenskontakte. Nicht-technische Informationen sind vor allem an die soziale Struktur der Zielgesellschaft gebunden.

Kombination aus technischen- & nicht-technische Informationen

Beide Teile der Informationsbeschaffungsphase können auf einem separaten Weg bei jeden Testfall kombiniert werden, um ausgezeichnete Penetrationstestergebnisse zu gewährleisten. Manchmal muss ein Unternehmen eine interne nicht-technische Struktur überarbeiten um so z.B. ein Problem zu beseitigen.

Angreifer können die nicht-technischen mit technischen Informationen kombinieren, um erfolgreich einen Angriff gegen das Zielunternehmen durchzuführen. Wir kombinieren die nicht-technischen mit den technischen Informationen in einem großen Verfahren um Ihre Infrastrukturen abzusichern.

Öffentliche Informationen

Alle Daten und Informationen, die wir in dieser Phase erfassen oder sammeln werden ohne Schwachstellen oder Exploits beschafft. Während der Erkundungsphase werden keine aktiven Cyber-Attacken oder Anrgiffe vorgenommen um Resultate nicht zu verfälschen.

Nach dem Informationsprozess in der Aufklärungsphase, wäre der nächste Schritt die Enumeration-Phase. Siehe die Enumeration Phaseninformationen im nächsten Schritt.

9.2 Enumeration (Attack Vectors)

The enumeration phase is the phase where the information of the reconnaissance phase will be in use the first time. The enumeration procedure impacts for example active actions taken by cyber attackers to gain system access and of course the important attack vectors or schemes. Information and Data captured through the reconnaissance phase build an review and overview about the target company. In special later test cases or topics the captured information plays a significant role in the enumeration or exploitation phase.

During enumeration phase, date and information will be systematically captured or tracked. In special cases individual systems, infrastructures or environments are complete identified by our security team during the enumeration phase simulation.

Enumeration ... ?!

Die Aufzählung Phase ist die Phase, in der die Information der Aufklärungsphase das erste Mal in Gebrauch genommen werden. Die Verfahrensauswirkungen sind zum Beispiel erste aktive Aktionen von Cyber Angreifern um Zugriff auf ein spezifisches System zu gewinnen oder um wichtigen Angriffsvektoren für Systeme in Erfahrung zu bringen. Informationen und Daten die durch die Aufklärungsphase in die Enumerationsphase übernommen werden bilden bei einer Überprüfung einen Überblick zu angegriffenen Zielgesellschaft. In späteren Simulationen oder

Testfällen bei speziellen Themen werden Informationen erfasst, die dauerhaft eine bedeutende Rollen in der Aufzeichnung und Auswertungsphase spielen.

Während der Enumerations Phase werden Informationen wie Datum und Zeitstempel systematisch erfasst um eine Verfolgung der Ereignisse zu gewährleisten. In einzelnen besonderen Fällen kann es vorkommen das durch die Prüfung bei Enumeration verfügbare Systeme, Infrastrukturen und Umgebungen vollständig von unserem Sicherheitsteam identifiziert werden.

Next Phase Exploitation

Nach der reconnaissance und enumeration -phase folgt die exploitation phase.

9.3 Exploitation

Die Exploitation Phase ist der dritte Schritt der Testsimulationsprozedur. In der Exploitation Phase ergreifen die Forscher und Sicherheitstester gezielt Maßnahmen um zero-day Sicherheitslücken oder bekannte Schwachstellen aktiv auszunutzen. Unsere Top Penetrationstester kombinieren verschiedene manuelle und automatische Verfahren während der Exploitation Phase um erfolgreiche Resultate zu erzielen.

Entwicklung - Exploits & Proof of Concepts

In der Exploitation Phase des Sicherheitstests werden unserer Sicherheitsforscher und Penetrationstester eigene Angriffsroutinen entwickeln um Filter zu umgehen oder um deren Sicherheitsmechanismen auszuhebeln. Währen der Exploitation Phase werden auch nicht autorisierte Zugriffe auf das System durch eigens entdeckte zero-day Schwachstellen simuliert. In der Exploitation Phase greifen unsere Forscher und Penetrationstester auch die Computersysteme mit eigenes entwickelter Software, Skripte oder Programmen an.

Öffentliche Bugs - Exploits & Proof of Concepts

Wir sind auch in der Lage, öffentlich bekannte Sicherheitsanfälligkeiten oder Berichte in unseren Sicherheitsprüfungen zu verwenden. Durch die kombinierte Nutzung von öffentlich verfügbaren Programmen, Proof of Concepts, Schadcodes oder Exploits steigt die Erkennungsrate beim aufdeckten von Sicherheitslücken und Schwachstellen in der jeweiligen Infrastruktur des Kunden. Unsere Priorität liegt dabei immer auf dem Fokus neue zero-day Schwachstellen zu identifizieren. Das Evolution Security Team beobachtet dauerhaft öffentliche Informationen über öffentlichte Anfälligkeiten oder Schwachstellen unserer Klienten und Kunden, um eine Absicherung zu gewährleisten.

Wiederholung der Reconnaissance oder Enumeration Phase

In der Exploitaion Phase haben die Forscher und Penetrationstester immer die Möglichkeit zurück in die Informationsbeschaffungsphase oder Enumerationphase zu springen, um neue Ziele zu erfassen oder auch Tests mit Gegebenheiten zu erweitern sowie erneut einzugeben.

Next Phase - Documentation

Nach der Exploitation-Phase, folgt die allgemeine Dokumentationsphase als Endphase der gesamten Simulation. Bitte lesen Sie auch über unsere Dokumentationsphase im nächsten Abschnitt der Programmseite.

9.4 Dokumentation

Die ausführliche Dokumentation stellt sicher, das die Probleme analytisch vom Hersteller (oder Entwicklerteam) reproduziert und rekonstruiert werden können. Die Dokumentation wird von den Mitarbeitern und Sicherheitsforschern bereitgestellt, die die Penetrationstests oder Sicherheitsuntersuchungen durchgeführt haben. Dort werden alle Sicherheitslücken und Funde bis ins Detail beschrieben, ebenfalls werden mögliche Lösungswege aufgezeigt. Unsere Berichte & Dokumentationen sind unterschiedlich aufgeteilt:

Detailierte Penetrationtests Berichte
Unsere Berichte sind unterschiedlich aufgeteilt:

Einleitung und Zusammenfassung
Hier werden Details bereitgestellt, beispielsweise über den Hersteller, dazugehörige Server/Dienste und natürlich über die Software oder das Produkt selbst.

Technische Details
Hier wird auf die gefundenen Sicherheitslücken eingegangen, die bei den Tests entdeckt wurden.

Ausführbare Beispiele
In diesem Teil werden weitere Informationen bereitgestellt, die zur Ausführung beitragen. Mit detailiertem "Proof of Concept" Code.

Lösungsvorschläge und Risikoanalysen
Der letze Teil der Berichte enthalten Lösungsvorschläge um die Sicherheitslücken zu schließen, sowie Rikioanalysen über die gefundenen Schwachstellen. Im letzen Schritt fügen unsere Mitarbeiter die Berichte zu einer finalen Dokumentation zusammen.

Nach der letzen Phase ... ?
After the last phase the evolution security team is ever responsible for security questions, problems, assistance to reproduce and of course a future cooperation. Werden Sie Teil unserers starken Sicherheitsnetzwerkes und stellen Sie durch permanente Prüfungen, Test und Analysen ihre Systeme auf die Probe.

Unternehmenssicherheitsreport (Einzelne Bereiche & komplettes Unternehmen)

Die Evolution Security GmbH bietet Ihnen einheitliche Unternehmenssicherheitsreports an, die speziell auf einzelne Infrastrukturbereiche wie z.B. das Rechenzentrum aufbauen. Zusätzlich bietet unser Unternehmen eine Komplettbewertung Ihres gesamten digital Unternehmensinfrastruktur an. Die Komplettbewertungen behinhalten Themen wie physische Sicherheit, Infrastruktur-Stabilitäts- und Integritätschecks, Zugangssicherheit und Überwachung & Monitoring. Weitere Details zum Thema, können Sie in unseren Servicedokumenten in Erfahrung bringen.

Management Zusammenfassung (Betriebsrat, Geschäftsführung, Investoren & Kunden)

Management Zusammenfassung (Betriebsrat, Geschäftsführung, Investoren & Kunden) Sie benötigen die Sicherheitsdokumentation als Zusammenfassung für unterschiedliche Abteilungen Ihrer Firma? Dies ist ebenfalls kein Problem, wir bieten Ihnen maßgeschneiderte Management Zusammenfassungen in der Sicherheitsdokumentation an, unabhängig davon, für welche Abteilung diese fällig ist. Ob für den Betriebsrat, die Geschaftsführung oder Investoren & Kunden, die

Evolution Security GmbH fertigt ein transparentes und auf die Abteilung zugeschnittenes Dokument an, um mögliche Mitarbeiter nicht mit überflüssigen, unverständlichen Details zu konfrontieren

10. Veranstaltungen & Konferenzen
10.1 IT-Sicherheit - Presentationen, Lektüren & Vorträge

Das Sicherheitssteam der Evolution Security GmbH hält erfolgreich öffentliche Präsentationen oder Vorträge, die in einem Zeitraum von jedem viertel Jahr überarbeitet werden um einzigartig zu bleiben. Die Vorträge sind sehr informativ gewählt für Forscher, Entwickler, Penetrationstester, Sicherheits-firmen um Angriffsmethoden, statische und dynamische Sicherheitssysteme, Umgehungsmethoden oder sichere Programmierung zu erlernen.

Unsere Firma bietet nicht nur Voträge und Präsentationen an, sondern auch Workshops oder Live-Hacking Shows für Veranstaltungen sowie Konferenzen. Wie auch in anderen Themen-bereichen, liegt der Schwerpunkt auf dem IT-Sicherheitsbereich.

Vorträge, Präsentationen & Workshops
Um einen Überblick auf die verschiedenen Schulungen und Workshops zu erhalten oder um Live-Hacking Shows auf Veranstaltungen zu geben, haben wir zusätzliche die folgenden Informationen für Sie zusammengestellt. Die meisten unserer Schulungen, Vorträge oder Live-Hacking Shows erfordern keine vorherigen IT-Kenntnisse im Bereich der Sicherheit. Nur wenn ein Workshop oder eine Präsentation mit fortgeschrittenem Titel markiert ist, benötigen Sie vorab ein technisches Wissen für das allgemeine Verständnis des Kunden bei Ausführung der Dienstleistung. Die Schulungen und Workshops nehmen durchschnittlich 1-2 Tag (e) in Anspruch nehmen und sind mit Pausen unterteilt. Die Live-Hacking Shows nehmen zwischen 30-60 Minuten in Anspruch unsere Vorträge und Präsentationen variieren zwischen 60 - 240 Minuten und sind somit ideal für Konferenzen, Weiterbildungen oder Schulungen.

Excellente Sprecher & neuste Themen
Wir bieten excellenten und exklusive Workshops in Bereichen wie Mobiltelefon Sicherheit, Software Schwachstellen, Applikation Sicherheitslücken oder Firewall und Filter Penetrationstests. Schauen Sie sich in Ruhe unsere Folien mit den Workshops und Kursen an und wählen Sie für Ihre Firma, eine Veranstaltung oder ein privates Team. Das Evolution Security GmbH Sicherheitsteam und unsere Forscher freuen sich auf Einladungen oder spezielle Anfrage für die teilnehmen auf Sicherheitskofnerenzen. Genießen Sie unsere Workshops, Vorträge oder Präsentationen und tauschen Sie sich mit den Experten unseres Unternehmens direkt vor Ort aus.

10.2 IT Security Workshops

Das Evolution Security Forschungsteam bietet verschedene Arten von IT-Sicherheit Workshops, in Kombination mit einem Training, vielen technischen Details, einer Buganalyse, Code review, Beispielcodes, Quelltexten, Bildern und exklusives Fachwissen. In der folgenden Tabelle werden alle wichtigen Workshops aufgeführt. Eine vollständige Liste der Workshops können Sie per Kontaktformular anfragen.

Note: Every month the workshop listing gets updates because of the internal company capacity.

https://www.evolution-sec.com/en/products/workshops-trainings

10.3 Live Hacking Shows & Veranstaltungen

Wir bei Evolution Security, sind immer auf dem aktuellen Stand und sind täglich auf der Suche nach neuen 0day Sicherheitslücken und neuen Angriffsvektoren. Unser Expertenteam verfügt über jahrelange praktischer Erfahrung und ihre Publikationen sind von rennomierten Firmen verteilt über die ganze Welt anerkannt.

Einige unserer Themen sind:

- Zero-Day Filter Bypass (Erweiterte Umgehungstechniken)
- Zero-Day Sicherheitslücken Forschung
- Erweiterte Rapid Penetration Testing
- Zero-Day Kernel Level Exploitation
- Erweitertes Malware Reverse Engineering

Alle demonstrierten Techniken während unserer Live Veranstaltungen, basieren auf einzigartigen Methoden, erdacht von unseren Mitarbeitern. Demnach ist es nicht notwendig auf öffentlich existierende Exploits und Tools zurückgreifen zu müssen. Unsere Live Veranstaltungen decken alles ab. Angefangen bei Netzwerkstrukturen, bishin zu System Level exploitation und Web Applikationen. Kontaktieren Sie uns, wir sind jederzeit offen für Fragen über unsere Trainings und Live Hackings Veranstaltungen.

11. Vulnerability Disclosure Policy

Wir überprüfen die Schwachstellen und senden die komplette Report an den Produktanbieter. Nach der Benachrichtigung und dem patch als work-around veröffentlichen wir die Beratung als stabile Referenz mit Autoren Information. Wir fordern auch CVE-IDs an und versuchen, unsere Informationen zu verschiedenen Quellen wie Nachrichten-Websites, Agenturen, Institutionen, Sicherheits-Monitoring-Services, Zeitschriften, RSS-Feeds oder mobile Blogs zu veröffentlichen. Unsere Kunden und Partner können hier die richtige Auswahl treffen, da wir drei flexible Standardmodule zur Verfügung stellen. Stille Offenlegung, Verantwortliche Offenlegung & vollständige Offenlegung.

11.1 Silent (Non-Public) Disclosure

Das stille Offenlegungsmodell unseres Unternehmens ist neu und nutzt regelmäßige die Anfälligkeitsaufklärungspolitik, diese wirkt sich auch auf einige wichtige Änderungen Prozeduren in der End-Phase aus. Die Sicherheitsanfälligkeiten in einem Programm bei unbeaufsichtigte Offenlegung werden nicht sichtbar, nachdem ein Patch von dem Herstellerunternehmen oder Produktverkäufer offenbart worden ist.

Im Rahmen des Programms "Stille Offenlegung" unterzeichnen die Forscher einen Sondervertrag mit der Wirkung eines nicht flexiblen Vertraulichkeits- oder Geheimhaltungsdokuments. Nach der Belohnung oder dem Patch können die Forscher nicht über den Sicherheitsvorfall sprechen. Die öffentliche Offenlegung des Bugs und der Ressourcen ist wegen der stillen Offenlegungspolitik nicht zulässig.

11.2 Full Disclosure

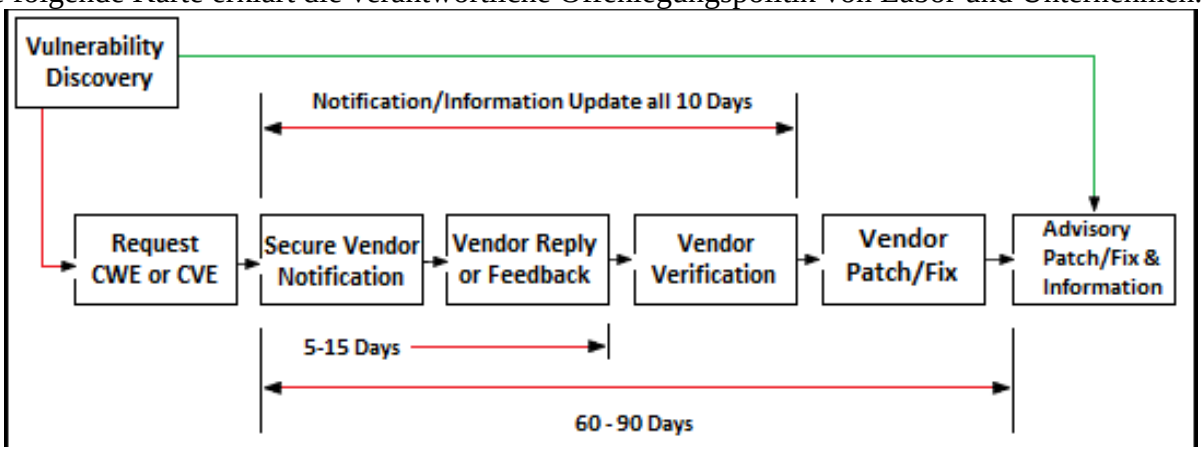
Die vollständige Offenlegung Modell unseres Unternehmens ist frei zu wählen. Manchmal sehen Verkäufer oder Hersteller einen Grund, die Informationen über Zero-Day-Schwachstellen und Bugs direkt zu offenbaren.

Das vollständige Offenlegungsmodell ermöglicht es dem Forscher oder Autor, seine Bug-Entdeckung direkt nach der Übergabe des internen Validierungsverfahrens an das Labors zu veröffentlichen.

List of Full Disclosure Bugs: (Example)
Vulnerability Laboratory - Independent Vulnerability Database (EU)
PacketStorm Security - Vulnerability Database (UK)
Offensive Security - Full Disclosure Exploit Database (US)
SCIP CH AG - Bulletin Notification System (EU)

11.3 Responsible Disclosure

Die folgende Karte erklärt die verantwortliche Offenlegungspolitik von Labor und Unternehmen.



12.2 - Domains (Dienste)

Unsere Firma besitzt mehrere soziale Netzwerk-Konten in facebook, flickr, google +, twitter oder youtube. Wir würden uns freuen wenn Ihr euch unserer Community anschliesst.

Evolution Security:

- https://www.evolution-sec.com
- https://www.vulnerability-lab.com
- https://www.government-lab.com

12.3 Partner & Kooperationen

Kontaktieren Sie uns für eine stabile & vertrauenswürdige Partnerschaft! Wir bieten eine kostenlose Banner-Austausch-Seite für aktive Sicherheitsprojekte, Dienstleistungen, Bugbounty-Programme, offizielle und rechtliche Websites oder Labore.

Unsere Partnerkategorien sind in 9 Teile aufgeteilt:

- Sponsorship
  (OFFICIAL PARTNERS & COORDINATION)
- Information Exchange Partnership
  (ID, ADVISORY & TECHNICAL/SPECIAL SUPPORT)
- Security Conference & Event Partnership
  (SUPPORT SPEAKERS, TALKS & PRESENTATIONS)
- Vulnerability Exchange Partners
  (BUG BOUNTY & COMMERCIAL REWARD PROGRAMS)
- Research Team Exchange Partnership
  (FEED UPDATES & COOPERATIVE COMPANIES)
- Vulnerability Disclosure Partnership
  (SOFTWARE/SERVICES/APPLICATIONS)
- Security Researcher Acknowledgment Partnership
  (HALL OF FAME & ACKNOWLEDGMENTS)
- Security Media & News Partnership
  (SECURITY NEWS & MAGAZINES)
- Trusted Security Community Partnership
  (SECURITY COMPANIES)

URL: (Vulnerability Laboratory) - www.vulnerability-lab.com/partner.php

Das „Evolution Security GmbH“ Unternehmen und das „Vulnerability-Laboratory“ beobachten langfristige Partnerschaften mit Herstellern, Kunden und Unternehmen, um auf Dauer optimale Ergebnisse zu erzielen.