Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

InfoGuard Hardening Services

Inhaltsverzeichnis

1 Management Summary

1.1 Ausgangslage

Unsere Erfahrung aus über 100 untersuchten Ransomware Vorfällen, sowie das Fachwissen unserer Ethical Hacker sowie Security Engineers zeigen uns deutlich, dass mit gezielten Hardening Massnahmen das Sicherheitsniveau Ihrer Infrastruktur signifikant erhöht wird. Die Boardmittel der Microsoftumgebung bietet eine Vielzahl an Möglichkeiten, die Resilienz zu steigern, ohne dabei zusätzliche Lizenzen beschaffen zu müssen. Im Gegenzug birgt die Komplexität dieser Umgebung das Risiko, durch unbedachtes Umsetzen solcher Massnahmen einen Businessimpact hervorzurufen. Der Aufbau von Expertise im Umgang mit diesen Hardeningmassnamhen ist daher entscheidend.

1.2 Lösungsbeschreibung

Unsere Hardening-Lösung stellt einen kontinuierlichen Prozess dar, der die Cyber Resilienz eines Unternehmens stärkt. Um einen einfachen Einstieg zu ermöglichen und gleichzeitig eine klare Struktur zu bieten, haben wir spezifische Module entwickelt, die gezielte Bereiche ansprechen. Jedes Modul beinhaltet klar definierte Massnahmen, die zur umfassenden Härtung der Kundenumgebung beitragen. Durch die schrittweise Umsetzung der Module verbessert sich die Cyber Resilienz des Unternehmens kontinuierlich.

Diese Module sind so konzipiert, dass sie gut in die IT-Organisation integriert werden können und in einem festgelegten Zeitrahmen umsetzbar sind. Durch die Modularität haben wir die Flexibilität, gemeinsam mit dem Kunden zu bestimmen, wo die Schwerpunkte gesetzt werden sollen. Unsere empfohlene Vorgehensweise besteht darin, zunächst die Basis-Module zu fokussieren, um die gesamte Organisation breit abzudecken, bevor wir uns dann in den spezifischen Bereichen mit den Advanced-Modulen vertiefen. So schaffen wir gemeinsam eine solide und anpassungsfähige Sicherheitsinfrastruktur.

2 Ihr Partner

2.1 InfoGuard – Cyber Security ist unsere Leidenschaft

InfoGuard ist spezialisiert auf umfassende Cyber Security. Unsere 360°-Expertise reicht von Cyber Defence Services und Incident Response Services über Managed Security & Network Solutions für IT-, OT- und Cloud-Infrastrukturen bis hin zu Services in den Bereichen Architektur, Engineering, Penetration Testing & Red Teaming sowie Security Consulting. Die Cloud-, Managed- und SOC-Services erbringen wir aus dem ISO 27001-zertifizierten und ISAE 3000 Typ 2 überprüften Cyber Defence Center in der Schweiz.

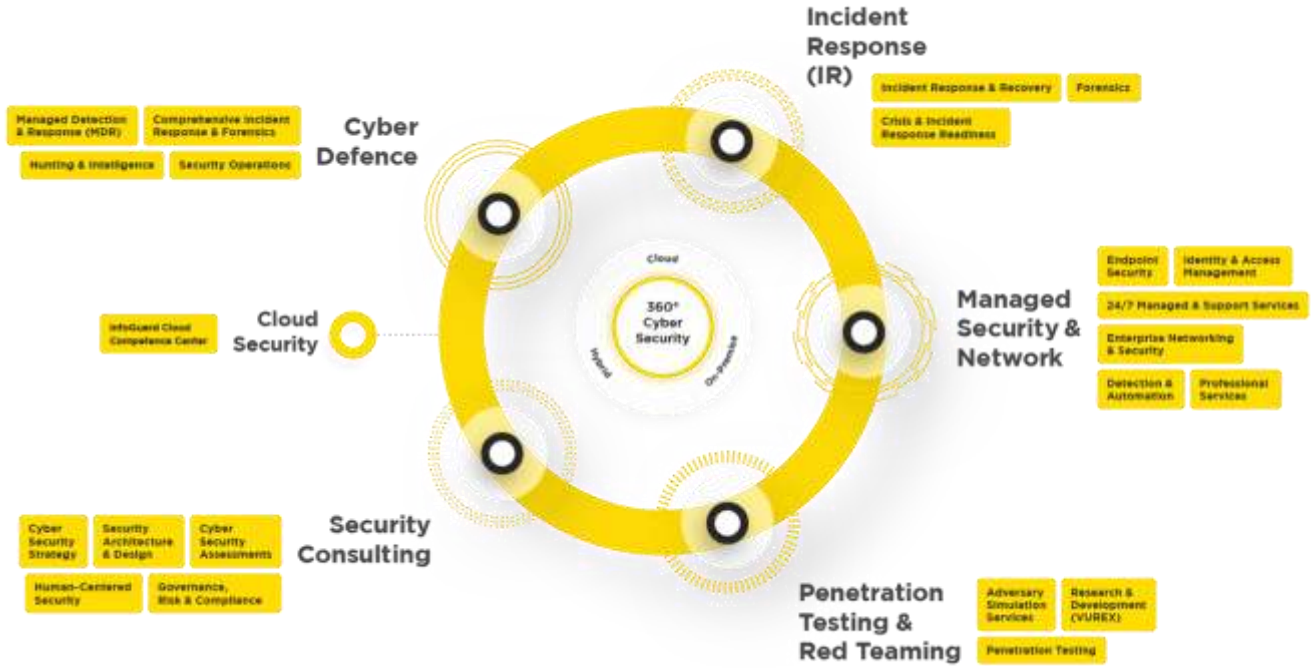
InfoGuard, mit Hauptsitz in Baar/Zug sowie Niederlassungen in Bern, München und Wien, schützt rund um die Uhr mehr als 700 Unternehmen in der Schweiz, Deutschland und Österreich. Dafür sorgen über 230 Sicherheitsexpert*innen. Zu den Kunden zählen namhafte Banken, Versicherungen, Industrieunternehmen, Energiedienstleister, Spitäler, Handelsunternehmen, Service Provider und Behörden. InfoGuard ist ISO/IEC 27001- sowie ISO 14001-zertifiziert, BSI-qualifizierter APT-Response-Dienstleister und Mitglied bei FIRST (Global Forum of Incident Response and Security Teams).

Unsere Partner

Um unseren Kunden eine optimale Lösung bieten zu können, arbeiten wir strategisch mit ausgewählten Herstellern zusammen. Unsere Kunden profitieren dabei von der langjährigen Zusammenarbeit, unserer breiten Erfahrung im Cyber Security und Netzwerkbereich sowie vom grossen Know-how unserer zertifizierten Partner.

Cyber Security Made in Switzerland

In der heutigen digitalen Welt ist Cyber-Sicherheit von entscheidender Bedeutung. InfoGuard steht für verlässliche, innovative Services und Lösungen, die Ihre Sicherheit und Ihr Vertrauen schützen. Mit unserem ganzheitlichen Ansatz, hochspezialisierten Mitarbeitenden, effizienten Prozessen und modernsten Technologien sorgen wir dafür, dass Sie heute und in Zukunft in der komplexen digitalen Welt sicher sind.



Cyber Defence

In der dynamischen, sich ständig verändernden Welt der Cyber-Bedrohungen ist es entscheidend, potenzielle Angriffe schnell zu identifizieren und zu bekämpfen – und zwar 24/7. Sämtliche Services werden aus dem ISO 27001-zertifizierten Cyber Defence Center (CDC) in der Schweiz erbracht.

Incident Response

Erfolgreiche Cyber-Angriffe können nie vollständig ausgeschlossen werden. Unser Computer Security Incident Response Team (CSIRT) steht Unternehmen im Ernstfall zur Seite und sorgt dafür, dass sie schnellstmöglich wieder handlungsfähig sind.

Managed Security & Network

Cyber-Sicherheit gelingt nur mit einem stabilen, zuverlässigen Fundament. Dazu entwickeln wir IT-Sicherheitsarchitekturen, die auf modernsten Netzwerk- und Sicherheitslösungen basieren. Durch umfassende Professional Services sowie 24/7 Managed Services gewährleisten wir den kontinuierlichen Schutz digitaler Infrastrukturen und die zuverlässige Verfügbarkeit.

Penetration Testing

Effektive Cyber-Sicherheit erfordert ein tiefes Verständnis der Methoden und Taktiken von Cyber-Kriminellen. Mit unserer Expertise im Bereich Penetration Testing & Red Teaming identifizieren wir nicht nur Schwachstellen, sondern entwickeln auch Tools und Verfahren, um diese zu erkennen, bevor potenzielle Angreifer sie ausnutzen.

Security Consulting

Professionelle Sicherheitsberatung ist unverzichtbar, um den vielfältigen Anforderungen gerecht zu werden – sei es im Bereich Strategie, Governance, Risk und Compliance, Architektur und Design, Security Assessments oder bei der Förderung einer sicherheitsbewussten Unternehmenskultur.

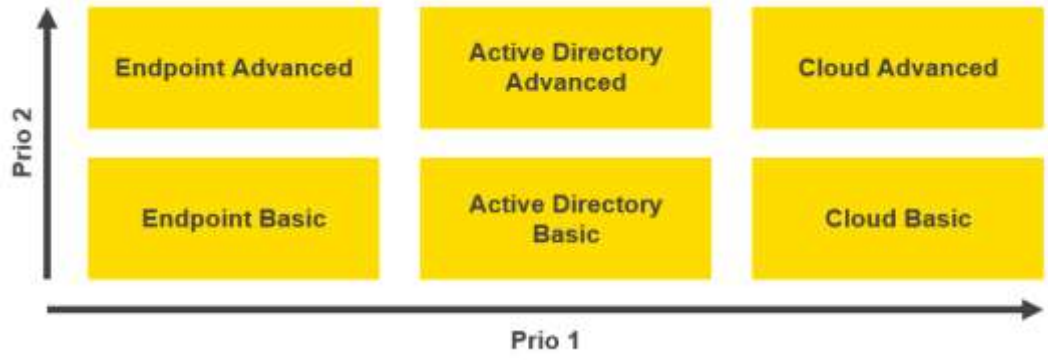
Cloud-Security

Umfassende Sicherheit und Expertise in der Cloud – von der Strategie, Architektur und Transition über die professionelle Umsetzung und den sicheren Betrieb bis hin zur kontinuierlichen Optimierung und dem reibungslosen Off-Boarding.

3 Beschreibung der offerierten Services

3.1 Übersicht Hardening Pakete

Hardening ist ein stetiger Prozess, der fortlaufend dazu beiträgt, die Cyber Resilienz eines Unternehmens zu steigern. Um hier einen einfachen Einstieg zu bieten - aber auch einen roten Faden zu haben - bieten wir im Rahmen eines Hardening Service Module an, die als einzelne Bausteine spezifische Bereiche adressieren. Diese Module enthalten klar definierte Massnahmen, die zur Gesamt-Härtung der Kunden-Umgebung beitragen. Je mehr der Module umgesetzt werden, umso besser wird damit die Cyber Resilienz der Unternehmung. Jedes Modul deckt dabei einen Teilbereich der Umgebung ab und ist so strukturiert, dass sie gut verdaubar für die IT Organisation sind, d.h. in einem definierten Zeitrahmen umsetzbar sind.
Dank der Modularität kann zusammen mit dem Kunden definiert werden, wo die Schwerpunkte gesetzt werden sollen. Die empfohlene Vorgehenweise ist dabei die Fokussierung auf die Basis Module und damit in die Breite der Organisation und danach die Vertiefung in den einzelnen Bereichen mittels den Advanced Modulen.
Die Massnahmen sind alle Built-In – es ist keine zusätzliche Investition getätigt werden (*ausgenommen Attack Surface Reduction ASR Rules).



Nachfolgend einige Beispiele von Härtungsmassnahmen, um ein besseres Verständnis über die möglichen Inhalte der einzelnen Module zu erhalten.

- «Block abuse of exploted vulnerable signed drivers»
  Diese Massnahme verhindert, dass eine Anwendung einen anfälligen signierten Treiber auf die Festplatte schreibt. Anfällige signierte Treiber von lokalen Anwendungen - die über ausreichende Berechtigungen verfügen – können ausgenutzt werden, um Zugriff auf den Kernel zu erhalten. Sie ermöglichen Angreifern, Sicherheitslösungen zu deaktivieren oder zu umgehen, was schließlich zu einem System-Compromise führt.

- «Block all office applications from creating child processes»
  Diese Massnahme verhindert, dass Office-Anwendungen untergeordnete Prozesse erstellen. Dazu gehören Word, Excel, PowerPoint, OneNote und Access.

- «Block Office applications from creating executable content»
  Diese Massnahme verhindert, dass Office-Anwendungen, einschließlich Word, Excel und PowerPoint, potenziell bösartige ausführbare Inhalte erstellen, indem sie das Schreiben von ausführbarem Code auf die Festplatte blockiert.

- Full Disk Encryption
  Bei dieser Massnahme geht es um die Implementation einer Full Disk Encryption. Dies stellt sicher, dass die Daten im Falle eines Verlusts sicher sind.

3.2 Beschreibung Prozess

3.2.1 Vorbereitung

Mit dem Kickoff startet die Zusammenarbeit im Zuge des Hardening Service. Ziel ist es einerseits, den Kundenbedarf abzuholen und die Massnahmen ideal auf seine Bedürfnisse abzustimmen. Andererseits werden die Rollen und Verantwortlichkeiten festgelegt. Ein weiterer, wesentlicher Punkt ist die Erläuterung des «Customer Enablement Process» - innerhalb dieses Prozesses werden die Hardeningmassnahmen abgearbeitet. Unser Ziel ist es, dem Kunden ein hohes Mass an Selbstständigkeit zu ermöglichen, ohne dabei auf professionelle Unterstützung verzichten zu müssen. Nachfolgend wird der Customer Enablement Prozess dargestellt.

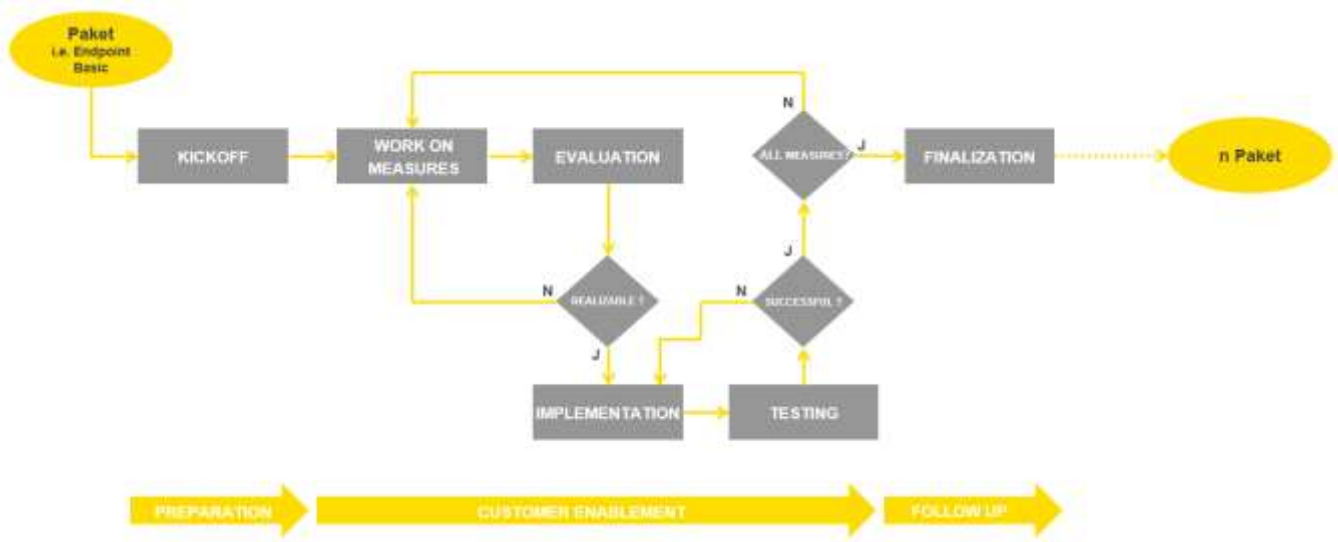


Abbildung 1: Customer Enablement Process

3.2.2 Befähigung des Kunden

Diese Befähigung wird durch das Befolgen des «Customer Enablement Process» bei der Umsetzung der Massnahmen erlangt. Nachfolgend sind die Teilschritte kurz zusammengefasst:

- Evaluation: Bei der Evaluation geht es darum sicherzustellen, dass die Massnahmen umgesetzt werden können. Dabei wird zwischen technischem und organisatorischem Impakt unterschieden. Beim technischen Impakt wird verifiziert, ob nach der Umsetzung mit technischen Einschränkungen zu rechnen ist und ob diese entsprechend in Kauf genommen werden können. Beim organisatorischen Impakt geht es im Vergleich dazu um die organisatorischen Einschränkungen und/oder deren Notwendigkeit zur Anpassung von bereits bestehenden Prozessen, Richtlinien und Weisungen.
- Implementation: Die eigentliche Umsetzung der Härtungsmassnahmen findet in diesem Schritt statt. Dieser Teilschritt kann, je nach Organisation des Kunden, den internen Change Prozess initiieren. Die Umsetzung erfolgt in bewährten Teilschritten Test, Pilot und volle Produktionsumgebung.
- Testing: Nach der Umsetzung der jeweiligen Massnahmen wird einerseits die Effektivität der Einstellung, andererseits das Verhalten in der Infrastruktur, überprüft. Ziel dieses Schritts ist es, sicherzustellen, dass der Betrieb von der Härtungsmassnahme möglichst wenig mitkriegt. Allfällige Abweichungen zur vorgängigen Verifizierung des technischen/organisatorischen Impakts sind zu vermerken.

3.2.3 Abschluss

Beim Abschluss finalisieren wir den Bericht, der die durchgeführten Massnahmen und die erzielten Ergebnisse zusammenfasst. Gemeinsam reflektieren wir über die erzielten Erfolge und stellen so sicher, dass die Sicherheitsmassnahmen optimal auf die Bedürfnisse des Kunden abgestimmt ist.

3.3 Verantwortlichkeiten

HS4M – Hardening Service for Microsoft				
	Projekt Manager	**Security Engineer**	**Manager**	**Subject Matter Expert**
Tasks und Aktivitäten **Beschreibung**	**InfoGuard**		**Customer**	
Vorbereitung				
Ziele definieren Festlegung der spezifischen Sicherheitsziele und -anforderungen in Abstimmung mit dem Kunden.	A	C	R	I
Abstimmung der Module Auswahl der Module basierend auf den individuellen Anforderungen.	A	R	I	C
Verantwortlichkeiten festlegen Klare Festlegung der Rollen und Verantwortlichkeiten sowohl seitens des Kunden als auch des Serviceanbieters.	A	R	I	C
Zeitplan festlegen Festlegung eines Zeitrahmens für die Umsetzung der verschiedenen Module.	A	R	I	C
Befähigung des Kunden				
Evaluation der Massnahme (organisatorisch) Sicherstellen, dass Massnahmen organisatorisch umgesetzt werden können.	I	C	A	R
Evaluation der Massnahme (technisch) Sicherstellen, dass Massnahmen technisch umgesetzt werden können.	I	C	A	R
Implementation der Massnahme Umsetzung der evaluierten Massnahmen gemäss Beschreibung im Massnahmenkatalog unter Berücksichtigung des potentiell vorhandenen, internen Change Prozess.	I	C	A	R
Testing Prüfen der Effektivität sowie des Verhalten innerhalb der Infrastruktur.	I	C	A	R
Updates am Massnahmenkatalog einfliessen lassen Updates am Massnahmenkatalog während der Erbringung des Hardening Service.	A	R	I	C
Abschluss				
Erstellung Bericht Erstellung eines Abschlussberichts, welcher die durchgeführten Massnahmen, die Ergebnisse sowie potentielle Abweichungen zur Evaluation dokumentiert.	A	R	I	C
Reflexion und Feedback Gemeinsame Reflexion, um sicherzustellen, dass die umgesetzten Massnahmen optiomal auf die Bedürfnisse des Kunden abstimmt sind.	A	R	I	C
Langfristige Strategie Diskussion über weitere Schritte zur langfristigen Sicherung der Unternehmensumgebung.	A	C	R	I