CYBER WERKSCHUTZ

Cyber Sicherheitsdienst

Umfassender Schutz Ihrer IT

LEISTUNGSBESCHREIBUNG

Cyber Werkschutz: Prävention und Monitoring

ENDPOINT DETECTION AND RESPONSE (EDR)

Überwachung von Windows, sowie MAC Systemen auf sicherheitsrelevante bzw. verdächtige Ereignisse, optional in Verbindung mit Endpoint Protection (Antivirus).

Ressourcenschonende Sensoren für Windows Systeme (Server und Clients) überwachen verdächtige Programm- und Benutzeraktivitäten auf den Geräten und streamen Ereignis- und Verhaltensdaten in Echtzeit in eine sichere Cloudumgebung in der europäischen Union. Dort werden die Daten kontinuierlich ausgewertet und Verdachtsfälle von den BWG Sicherheitsexperten näher analysiert. Bei bestätigten Erkennungen werden Sie vom BWG Security-Team kontaktiert und erhalten Empfehlungen für Gegenmaßnahmen.
Das Modul Endpoint Detection and Response (EDR) steht für folgende Geräte zur Verfügung:

- Aktuelle Windows & Mac Computer Workstations (Standalone oder inkl. Endpoint Security)
- Aktuelle Windows Server (Standalone oder inkl. Endpoint Security)

VULNERABILITY SCAN

Wöchentliche automatisierte Überprüfung der aus dem Internet erreichbaren Systeme auf Schwachstellen (Schwachstellenanalyse).

Mit Hilfe eines cloudbasierten Schwachstellenscanners (Server Standort: Europäische Union) werden aus dem Internet erreichbare Systeme in regelmäßigen Abständen (1 x pro Woche) auf Schwachstellen überprüft.
Identifizierte Schwachstellen werden in Form eines E-Mail Reports mitgeteilt. Das BWG Security-Team unterstützt mit Hinweisen und ggf. Empfehlungen (z. B. zur Konfiguration einer vorhandenen Firewall oder vergleichbaren Abwehrmaßnahmen).
Die Behebung von Schwachstellen ist ausdrücklich nicht Bestandteil des BWG Cyber Werkschutz.

DEEP WEB MONITORING

Überwachung der E-Mail Domain(s) auf Data Breaches.

Für die Überwachung der E-Mail Domains werden kontinuierlich und automatisiert unterschiedliche Datenquellen mit Hilfe einer kommerziellen Datenbank ausgewertet. Die bei der Initialisierung des Service identifizierten E-Mail-Adressen und zugehörige Daten der überwachten E-Mail Domains werden im Rahmen des Onboarding-Prozesses an den Kunden übermittelt. Sind bei künftigen Data Breaches weitere E-Mail-Adressen betroffen, informiert das BWG Security-Team über den Vorfall.

SUSPICIOUS TRAFFIC DETECTION

Betrieb eines passiven Sensors im Kundennetzwerk zur Identifikation von z. B. Portscans im internen Netzwerk.

Die Suspicious Traffic Detection erkennt im Rahmen bestimmter Systemgrenzen z. B. Portscans im Kundennetzwerk. Die hierfür erforderliche Auswertung des Netzwerkverkehrs erfolgt über einen passiven IDS-Sensor auf Basis eines Linux-basierenden Kleinstrechners (Hardware) bzw. einer virtuellen Maschine (Appliance). Der IDS Sensor erhält eine IP-Adresse aus dem / den zu überwachenden Netzwerk(en). Erkannte Portscans und andere Auffälligkeiten werden via Syslog-Protokoll an den Monitor Probe übertragen und von dort an das BWG Security-Team weitergeleitet. Zu Wartungszwecken (Software Updates) und für die Nachrüstung künftiger Funktionen, wird der Sensor über eine gesicherte Verbindung mit dem Wartungsnetzwerk von BWG verbunden.

FAILED LOGIN DETECTION UND SECURITY GROUP MONITORING

Überwachung von maximal 2 Domänencontrollern auf fehlgeschlagene Administratoren Logins. Überwachung der Administratorengruppe auf maximal 2 Domänencontrollern auf Änderungen, z. B. Hinzufügen / Entfernen von Benutzern zu dieser Gruppe.

Für die Erkennung fehlgeschlagener Anmeldeversuche von Administratoren am Active Directory sowie zur Überwachung der Administratoren Gruppe im Active Directory auf Änderungen müssen die entsprechenden Attribute in das Ereignis-Log des / der Domänencontroller geloggt werden. Die Auswertung und Weiterleitung erkannter Ereignisse erfolgt über einen Windows Software Agenten. Der Monitor Probe ist darüber hinaus als Remote-Syslog Server konfiguriert und leitet zusätzlich zu den Alarmen aus der Failed Login Detection und dem Security Group Monitoring auch Informationen aus der Suspicious Traffic Detection an das BWG Security-Team weiter.

SECURITY HOTLINE UND SUPPORT

Hotline und Supportunterstützung für Ihre Sicherheit.

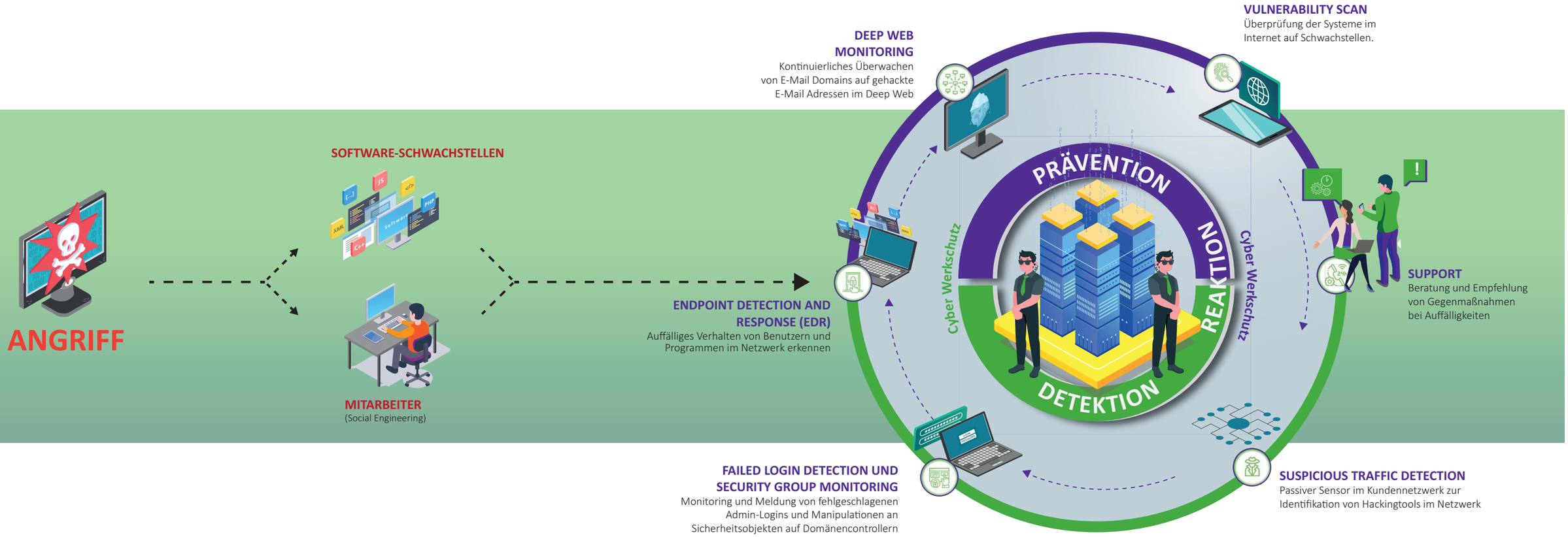
Das BWG Security-Team unterstützt durch Beratung im Fall einer Bedrohung und hilft bei der Einleitung geeigneter Gegenmaßnahmen.

DER ENTSCHEIDENDE GESCHWINDIGKEITSVORTEIL BEI ANGRIFFEN GEGEN IHR UNTERNEHMEN

Der BWG Cyber Werkschutz kombiniert **künstliche Intelligenz** mit unseren **menschlichen Spezialisten**

CYBER WERKSCHUTZ

BWG Systemhaus



DIE AUFGABE DES BWG CYBER WERKSCHUTZES

Die wichtigste Aufgabe eines Sicherheitsdienstes (Werkschutz) ist es, ein Unternehmen, seine Mitarbeiter und Einrichtungen vor Schäden zu schützen. Dazu gehören vorbeugender Brandschutz, Pforten- und Streifendienste und die Videoüberwachung des Geländes und der Anlagen. Sobald Auffälligkeiten oder Unregelmäßigkeiten beobachtet werden, informiert der Werkschutz unverzüglich die Entscheider im Unternehmen. So kann auf Bedrohungen frühzeitig reagiert werden und Unternehmenswerte sowie Mitarbeiter können geschützt werden.

Nach diesem Vorbild wurde der „BWG Cyber Werkschutz“ entwickelt. Er übernimmt damit die Aufgaben, die herkömmliche Sicherheitstechniken kaum mehr übernehmen können: Die Gefahrenabwehr in den Bereichen der Informationstechnik und Unterstützung des IT Personals. Dazu gehören beispielsweise die Überwachung im Falle von gezielten Hacking- oder Sabotageangriffen auf Endgeräte, Manipulationen an Sicherheitseinrichtungen oder die Täuschung von Mitarbeitern mit Hilfe von Social Engineering Methoden.

IHR PERSÖNLICHER CYBER SICHERHEITSDIENST

Der BWG Cyber Werkschutz arbeitet wie eine Kombination aus Alarmanlage, Videoüberwachung und Wachmannschaft: leistungsfähige Software Technologien werden mit der fundierten Erfahrung unserer Sicherheitsexperten erweitert.
In Echtzeit wird in der Flut der täglich auflaufenden Informationen die wirklich sicherheitsrelevanten Ereignisse identifiziert und gleichzeitig mit unterschiedlichen Informationsquellen abgeglichen.

Die durch diese Korrelation gewonnenen Erkenntnisse werden von erfahrenen Security Engineers interpretiert und konkrete Verdachtsfälle so aus dem allgemeinen „Rauschen“ herausgefiltert.

Diese Kombination aus „Man and Machine“ ist es, die den entscheidenden Geschwindigkeitsvorteil bei der Früherkennung gezielter Angriffe liefert.

PERFEKTER SCHUTZ FÜR KLEINE UND MITTLERER UNTERNEHMEN

Kritische Ereignisse, z. B. bestätigte Angriffe oder Ausführung gefährlicher Programme oder Skripte, werden während unserer Servicezeiten direkt an einen Entscheider Ihrer Organisation gemeldet.
Je nach vereinbartem Servicelevel unterstützen Sie unsere Sicherheitsexperten auch bei der Analyse des Vorfalls und bei der Einleitung von Gegenmaßnahmen.

Der Cyber Werkschutz ist gerade für kleine und mittlere Unternehmen attraktiv, die sich hochbezahlte Sicherheitsexperten in der Regel nicht leisten können. Der Cyber Werkschutz steht Ihrem Unternehmen als Service zur Verfügung – Sie bezahlen nur für die tatsächlich überwachten Geräte in Ihrem Netzwerk. Und das zu einer geringen monatlichen Gebühr.

BWG SYSTEMHAUS GRUPPE

IT Kompetenz im Großraum Karlsruhe und Stuttgart – seit 1980

DIE BWG SYSTEMHAUS GRUPPE AG

mit Zentralsitz in Ettlingen bei Karlsruhe und einer Niederlassung in Stuttgart, wurde 1980 in Karlsruhe gegründet und steht seither für Kontinuität und Innovation in einer rasanten Branche.

Um die über 1500 Kunden und Anwender optimal zu bedienen, wurden die Aktivitäten der BWG in einzelne Unternehmen mit gezielt ausgebildeten Mitarbeitern gegliedert:

Die BWG Informationssysteme GmbH bietet innovative Lösungen im Netzwerkumfeld wie Serversysteme, Speichernetzwerke, VPN-Anwendungen und hochspezialisierte Security-Konzepte. Individuell konfigurierte Industrie PCs und Mobile-Computing sind weitere Stärken.

Die BWG Medizinsysteme GmbH hat sich auf IT-Anwendungen im Gesundheitswesen spezialisiert. Praxisverwaltungssysteme für niedergelassene Ärzte und medizinische Versorgungszentren werden um Lösungen für die digitale Spracherkennung, Archivierung und digitale Röntgenanwendung ergänzt.

UNSERE LÖSUNGEN

BWG IT-Infrastructure
Wir konzipieren und implementieren eine speziell auf Ihre Bedürfnisse zugeschnittene Netzwerk- / Server und Cloud-Infrastruktur.

BWG Medical IT
Sie kümmern sich um Ihre Patienten – wir kümmern uns um Ihre IT.

BWG IT-Security
IT-Sicherheitskonzepte? Computerviren? Datenverlust? Wir machen Ihr Netzwerk sicher!

BWG Managed IT-Services
Supportunterstützung oder komplettes Outsourcing der wichtigsten Komponenten Ihrer IT-Infrastruktur

SPRECHEN SIE UNS AN!
info@bwg.de

IT wird jetzt einfach

ETTLINGEN
BWG Systemhaus Gruppe AG
Nobelstraße 22
76275 Ettlingen

Tel: +49 (0) 7243 7744-0
Fax: +49 (0) 7243 7744-900

E-Mail: info@bwg.de

STUTTGART
BWG Systemhaus Gruppe AG
Zettachring 2
70567 Stuttgart

Tel.: +49 (0) 711 13277-0
Fax: +49 (0) 711 13277-520

E-Mail: info@bwg.de

bwg.de

Stand 12.2020