ISPIN AG ZURICH
swiss made security.®
Member of CymbiQ Group

CSIRT Services

Präventiv handeln. Sofort reagieren. Cyber-Resilienz stärken.

Die Zahl der Cyberangriffe steigt ständig. Früher oder später trifft es auch Ihr Unternehmen. Schützen Sie sich, aber seien Sie auch darauf vorbereitet, dass Attacken Ihren Geschäftserfolg bedrohen können. Erhöhen Sie Ihre Cyber-Resilienz mit den CSIRT-Services von ISPIN.

Irgendwann trifft es jedes Unternehmen. Haben Sie sich schon einmal die Frage gestellt, welchen Schaden ein Angreifer in Ihrem Unternehmen anrichten könnte? Das hängt nicht in erster Linie von der Art der Attacke – Ransomware, Datendiebstahl oder Insider-Delikt – ab. Massgeblich für die Höhe des Schadens ist vielmehr, ob und wie gut Ihr Unternehmen auf einen solchen Zwischenfall vorbereitet ist und wie effizient Sie darauf reagieren können. Unser zertifiziertes CSIRT (Computer Security Incident Response Team) schützt Sie davor und sorgt dafür, die Auswirkungen gering zu halten, sollte doch einmal ein Angriff erfolgreich sein. Mit den ISPIN CSIRT-Services erhöhen Sie proaktiv die Cyber-Resilienz Ihres Unternehmens und bewahren es vor Schäden durch Cyberangriffe.

Ihre Vorteile auf einen Blick

- 7/24 Zugang zu unserem erfahrenen, zertifizierten Security Incident Response Team (CSIRT)
- Umfassendes präventives Servicepaket mit Praxischecks, Analysen, Monitoring und Simulationen
- Regelmässiges Security Intelligence Briefing inkl. Anpassungsvorschlägen
- Verbesserung der Effizienz und Effektivität, um auf Cyber Incidents zu reagieren
- Erhöhung der Cyber-Resilienz Ihres Unternehmens
- Sofort verfügbar, ohne Installationen

Drei Säulen. Ein Team. Mehr Sicherheit.

Die ISPIN CSIRT-Services bewahren Sie und Ihre Organisation vor dem Worst-Case, vor massiven Schäden durch Cyberangriffe. Dabei sind wir nicht nur im Ernstfall für Sie da, sondern erhöhen den Schutz Ihres Unternehmens auch mit einer ganzen Reihe präventiver Massnahmen. Unser CSIRT-Servicepaket – Ihr Schutzdach vor Cyberangriffen und deren Auswirkungen – setzt sich aus drei Säulen zusammen und stellt Ihnen ein Team aus zertifizierten Experten mit langjähriger Erfahrung in der Analyse und Behandlung von Cyber Incidents zur Seite. Das ISPIN CSIRT ist akkreditiertes Mitglied des Forum of Incident Response and Security Teams (FIRST) und stellt damit einen weltweit anerkannten Qualitätsstandard sicher.

PLANUNG macht den Unterschied

Gute Planung verhindert Katastrophen

Planen, wie es laufen soll: Start-Workshop
Das Service Setup besteht aus einem initialen Workshop zusammen mit unserem Security Incident Response Team. Dabei machen wir uns ein Bild über Ihre technische und organisatorische Infrastruktur und erarbeiten uns ein grundlegendes Verständnis Ihrer Geschäftsabläufe. Gemeinsam definieren wir die entsprechenden Kontakte, Informationskanäle und Prozesse und erstellen einen Servicekalender.

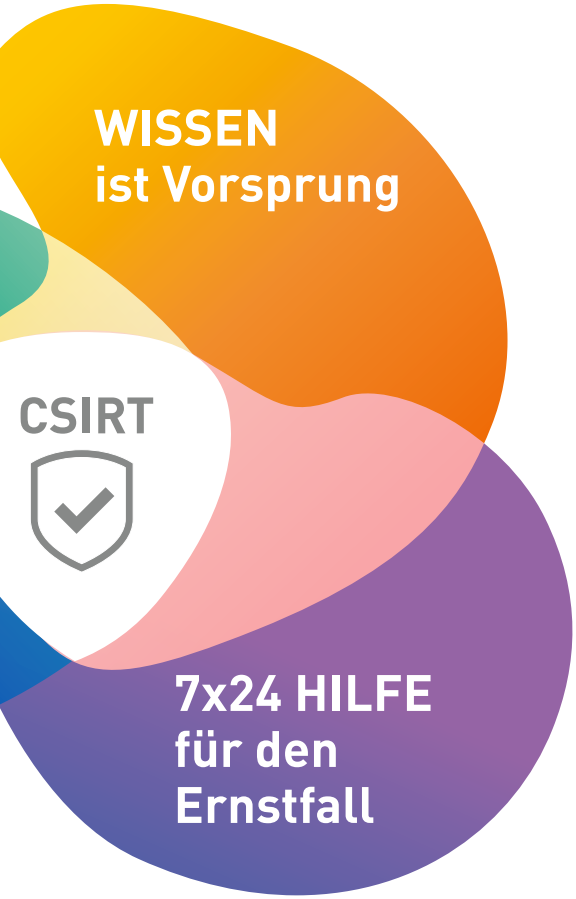
Planen, wie reagiert werden soll: Incident Response Planning (IRP)
Eine umfassende Planung macht den Unterschied zwischen einem einfachen Vorfall und einer Katastrophe. Daher überprüfen unsere Experten Ihre bestehenden Incident-Response-Pläne für verschiedene Szenarien. Sie haben noch keine solche Pläne? Kein Problem. Aus unserer umfassenden Sammlung stellen wir Ihnen die für Sie relevanten Pläne zur Verfügung und passen diese spezifisch Ihrer Organisation an.

Mehr Wissen ist besserer Schutz

Wissen, wie Ihr Team im Ernstfall reagiert: Incident Response Exercises
Für jede Art von Notfallplan gilt: Er ist nur so gut, wie er in der Praxis funktioniert. Deshalb führen wir gemeinsam mit Ihrem Security-Team Simulationen mit den verschiedenen Threat-Szenarien durch. Wir analysieren die Ergebnisse und helfen Ihnen, präventiv allfällige Lücken und Schwachstellen zu schliessen.

Wissen, welche Lücken Angreifer nutzen: Attack Surface Monitoring
Eine wirksame Cybersecurity-Strategie basiert darauf, die eigenen Schwachstellen zu kennen. Zu den häufigsten Angriffsflächen von Angreifern gehören bekannte Schwachstellen in Betriebssystemen. Aus diesem Grund scannen wir Ihre Umgebung kontinuierlich. Wir informieren Sie regelmässig über kritische Schwachstellen und geben Ihnen Empfehlungen zu deren Behebung. Damit reduzieren Sie proaktiv die technische Angriffsfläche nach aussen deutlich.

Wissen, wie Ihre Benutzer agieren: Phishing Simulation
Der Mensch ist das schwächste Glied in der (Cyber-)Verteidigungskette – weil er sich der Gefahren einfach nicht bewusst ist. Deshalb gilt es, sich dem Benutzerverhalten und dem Bewusstsein im Umgang mit Cyberrisiken besonderes aufmerksam zu widmen. Wir führen in regelmässigen Abständen simulierte Phishing-Angriffe durch und analysieren das Ergebnis. Diese Ergebnisse helfen Ihnen, das Verhalten der Benutzer zu beeinflussen und somit das Risiko deutlich zu reduzieren. Damit werden Ihre Benutzer vom schwächsten Glied zu einem wichtigen Verbündeten der Cybersecurity-Strategie.



Wissen, was der Gegner tut: Darkweb-Monitoring
Cyberangriffe kommen nicht aus dem Nichts. Sie folgen einem bestimmten Muster der Vorbereitung und Informationsbeschaffung. Diese Vorbereitungen finden in einem Teil des Internets statt, der normalerweise verborgen bleibt – dem sogenannten Dark- (oder auch Deep-)Web. Unsere Experten überwachen diese verborgenen Kanäle laufend. Dadurch sind sie in der Lage, Sie und Ihr Unternehmen über relevante Vorgänge zu informieren.

Wissen, wenn sich etwas ändert: CSIRT Ad-hoc-Report
Stösst unser Team im Zuge seiner Überwachungsmassnahmen auf Auffälligkeiten oder verdächtige Aktivitäten, benachrichtigt es Sie durch einen Ad-hoc-Report innerhalb von 24 Stunden. Dieser enthält Hintergrundinformationen über die festgestellte Bedrohung und Empfehlungen, wie dieser begegnet werden kann, zum Beispiel:

- Die Feststellung einer von aussen sichtbaren, als kritisch einzustufenden technischen Schwachstelle.
- Das Auftauchen von Benutzer- oder anderen Informationen Ihrer Organisation im Dark Web.
- Informationen zu neuen Cyberbedrohungen, inklusive «Zero-Day» oder neuartigen Angriffsmethoden.

Wissen, was sich entwickelt: CSIRT Intelligence Briefing
Die Bedrohungslage verändert sich ständig. Fast täglich werden neue Methoden oder bisher unbekannte Schwachstellen bekannt. Unsere Experten verfolgen die Entwicklung laufend und nehmen entsprechende Analysen vor. Neben den Ad-hoc-Reports erhalten Sie quartalsweise einen Intelligence-Bericht mit relevanten Informationen und Trends für Ihren Industriesektor. Dieser hält Vorgänge und Aktivitäten aus dem vergangenen Quartal fest. Zusätzlich liefert er Informationen über die Entwicklung von relevanten Cyberbedrohungen und über deren Hintergründe. Unser CSIRT bespricht den Report mit Ihnen und nimmt bei Bedarf Anpassungen am Servicekatalog vor.

Schnelle Hilfe im Notfall ist weniger Schaden

Wenn es passiert ist: 7x24 Incident Hotline 0848 800 017
Über den ISPIN CSIRT-Service erhalten Sie direkten 7x24 Zugang zu unserem Cyber Defense Team. Egal, ob Sie eine verdächtige Malware untersuchen lassen wollen oder in Ihrer Umgebung verdächtige Vorgänge feststellen – unsere Experten übernehmen die Analyse und helfen Ihnen bei den notwendigen Schritten. Ist bereits ein kritischer Zwischenfall eingetreten, dann unterstützen wir Ihren Krisenstab bei der Bewältigung, führen Analysen durch, schlagen Sofortmassnahmen vor und begleiten Sie, bis der Service wiederhergestellt ist:

- Wir spüren den Angriff auf, dämmen ihn schnellstmöglich ein und verhindern eine Ausbreitung.
- Wir sorgen dafür, dass Ihr Betrieb rasch wieder normal läuft.
- Wir analysieren den Vorfall und setzen gemeinsam mit Ihnen Optimierungen um.

Schnell und unkompliziert

Schnelle Hilfe erhalten Sie nicht nur bei unserer Incident Hotline. Sie können auch alle anderen CSIRT-Services rasch nutzen. Innerhalb weniger Tage oder bei Bedarf innerhalb von Stunden stellen wir Ihnen das umfassende Security-Paket zur Verfügung. Sie benötigen dafür weder Hardware, noch müssen Sie Software installieren. Wir sorgen dafür, dass Ihr Unternehmen unter dem Schutzdach unserer drei Security-Säulen die Risiken minimiert und vor Schäden bewahrt wird.

Cyber-Security – Swiss made und auf Ihre Bedürfnisse zugeschnitten.

ISPIN ist ein führender Schweizer Anbieter für Lösungen in Cyber Security und Cyber Risk Resilience®.

Kunden profitieren von einem lückenlosen Spektrum an Beratungs- und Lösungskompetenz: Security Awareness & Culture, Governance, Risk & Compliance (GRC) gehören ebenso dazu wie Cyber Defense Services, Cloud Security Services und Sicherheitsinfrastrukturen.

Mehr als 150 Kunden aus allen Segmenten der Privatwirtschaft und der öffentlichen Hand vertrauen ISPIN. Im modernsten Cyber Defense Center der Schweiz betreibt und überwacht ISPIN rund um die Uhr die Infrastrukturen von namhaften Unternehmen, Organisationen und Behörden.

Das sicherste Angebot auf einen Blick.

Incident Response Retainer	Basic	Compact	Premium	Protect
Start-Workshop	■	■	■	■
7x24 h Incident Response Hotline	■	■	■	■
CSIRT Ad-hoc-Report	■	■	■	■
CSIRT Intelligence Briefing	■	■	■	■
Stundenpool	n. A.	40	80	120
Attack Surface Monitoring	opt	■	■	■
Dark Web Analyse	opt	■	■	■
Incident Response Planning (IRP) Review oder Bereitstellung von bis zu 5 IRP Scenario Playbooks	opt	opt	■	■
Incident Response Exercise 2 Tabletop Exercises à je 4h	opt	opt	■	■
Phishing Simulation 2-mal jährlich, inkl. Analyse & Besprechung	opt	opt	opt	■

Sie benötigen kurzfristig Hilfe:

Ihre Incident Response Hotline: 0848 800 017

Wollen Sie mehr über unsere Cyber Defense Services erfahren?
Wir beraten Sie gerne: marketing@ispin.ch

ISPIN AG
Grindelstrasse 6
CH-8303 Bassersdorf
Tel.: +41 44 838 31 11
www.ispin.ch

Mitglied von:

FIRST Improving Security Together