

Das Incident Response-Team (IRT)

Wenn jede Sekunde zählt: Schnelle Hilfe bei IT-Sicherheitsvorfällen



Incident Response – Wie reagierst Du auf einen Sicherheitsvorfall?

Ein Cyber Angriff kann jedes Unternehmen treffen. Es ist nicht mehr eine Frage des „Ob“ sondern des „Wann“. Ganz egal wie groß Dein Unternehmen ist, in welcher Branche Du agierst oder wie hoch Dein Umsatz ist – den Hackern ist das egal. Ein Cyber Angriff kommt dann, wenn Du ihn am wenigsten erwartest. Und dann ist schnelles Handeln angesagt: Je besser Du auf einen Cyber Vorfall vorbereitet bist, desto höher ist die Chance, Schaden zu minimieren.

Incident Response (IR), also die Reaktion und die damit verbundenen Maßnahmen auf einen IT-Sicherheitsvorfall, ist ein Grundpfeiler der IT-Sicherheit eines modernen Unternehmens. Der Aufbau eines eigenen Incident Response Teams (IRT) ist dabei äußerst zeit- und ressourcenintensiv. Doch was, wenn der Ernstfall wirklich eintritt? Du solltest Dir folgende Fragen stellen, um sowohl Präventivmaßnahmen ergreifen zu können als auch für den akuten Sicherheitsvorfall gewappnet zu sein:

- Ist Dein Unternehmen auf einen IT-Sicherheitsvorfall vorbereitet?
- Gibt es Pläne, damit Du auf die wahrscheinlichsten Angriffsszenarien adäquat reagieren kannst?
- Hast Du bereits eine Simulation eines Sicherheitsvorfalls durchlaufen – inklusive Krisenmanagement und über alle Hierarchie Ebenen hinweg?

- Weißt Du, an wen Du Dich wenden musst? Hast Du IT-Spezialisten für alle Arten von Sicherheitsvorfällen an der Hand?
- Hast Du sämtliche Richtlinien für den Krisenfall ausgearbeitet mit Aktionsplänen und Prozessen, den zugeteilten Rollen und festgelegten Workflows?
- Fühlst Du Dich für den Fall eines IT-Sicherheitsvorfalls gut vorbereitet und gewappnet?

Ein Cyber Angriff ist immer mit vielen Unsicherheiten verbunden. Damit Du möglichst effizient und zielführend auf einen akuten Angriff reagieren kannst, bedarf es einer gründlichen Vorbereitung und Abwehr-Strategie, um möglichst schnell wieder handlungsfähig zu sein.

Das Incident Response Team (IRT)

Die Verantwortung für die Reaktion auf einen akuten Sicherheitsfall trägt meist ein dediziertes **Incident Response Team**, dass sowohl aus internen, externen oder aus einer Mischung beider Ressourcen bestehen kann. Das Team umfasst meist Sicherheitsspezialisten, IT-Experten aber auch Fachleute aus den Bereichen Unternehmenskommunikation sowie gegebenenfalls Mitarbeiter aus der Geschäftsleitung und der Personalabteilung. Ganz gleich, wie Dein Unternehmen aufgestellt ist: Deine Mitarbeiter sollten alle Maßnahmen gut vorbereitet haben und genau Bescheid wissen, damit im Ernstfall jeder weiß, was zu tun ist, ohne dass eine langwierige Organisation im Akutfall notwendig ist.

Der **Incident Response Service** von pco hilft Dir dabei, gezielt auf Cyber Security Incidents reagieren zu können, um eine schnelle Wiederherstellung Deiner existentiellen Geschäftsprozesse zu sichern.

Im Falle eines Angriffs unterstützen wir Dich bei der Analyse und der Bereinigung der betroffenen Systeme. Außerdem unterstützt das IRT auch bei der Wiederanlaufplanung Deiner IT-Services und analysiert den Incident parallel weiter, um mögliche Folgen abschätzen zu können. Zudem werden die Ursachen tiefer analysiert, um Dir Maßnahmen aufzuzeigen, wie Du Dein Unternehmen in Zukunft besser schützen kannst.

Um für zukünftige Vorfälle vorbereitet zu sein, erstellen wir anschließend ein Runbook bzw. einen Wiederherstellungsplan mit einer Übersicht über alle zu ergreifenden Schritte ebenso über die Zuständigkeiten in Deinem Unternehmen.

Und so geht es los: Das pco IRT-Onboarding

Um bei kritischen Sicherheitsvorfällen schnell und effektiv reagieren zu können, müssen wir sicherstellen, dass wir mit Deinen Systemen, Prozessen und Richtlinien vertraut sind. Der Gesamtüberblick über Deine IT-Infrastruktur, Deine Sicherheitsprotokolle und Ansprechpartner hilft uns dabei, uns nahtlos in Deinen Incident Response Plan zu integrieren, um Deine Systeme und Daten zu schützen.

Im Rahmen eines Onboardings hast Du zunächst die Möglichkeit, Dir einen Gesamtüberblick über Deine Geschäftsprozesse in Verbindung mit Deiner IT geben zu lassen: Kennst Du die Zusammenhänge zwischen Deinen wichtigen Geschäftsabläufen und Deiner IT-Landschaft und hast Du diese an Deine Ziele und geschäftlichen Anforderungen ausgerichtet?

Das Onboarding unseres Incident Response Teams beginnt mit einem gemeinsamen Workshop und der Ausarbeitung eines IRT-Steckbriefes. Im Anschluss können wir mit dem Incident Response Service in Deinem Unternehmen starten und Deine Security Maßnahmen auf Basis des sicheren Fundamentes perspektivisch weiterentwickeln.

IT Service Portfolio [\(Video\)](#)



Zusammenhänge Deiner Geschäftsabläufe und IT-Landschaft unter Berücksichtigung Deiner geschäftlichen Ziele.

Das sichere Fundament



Weiterentwicklung Deiner Security Maßnahmen auf Basis des sicheren Fundaments.



Onboarding

Workshop & Ausarbeitung eines IRT-Steckbriefs

Unsere Vertragsbausteine im Detail

| | | |
|-------------------|---|-----------------------------|
| IRT Basis Service | 24x7 IRT Hotline | |
| | Incident-Log Manager | |
| | IRT Manager Krisenmanager Ermittlungsleiter | |
| | IRT Analyse Hardware | EDR Lösung |
| | IRT Manager Krisenmanager Ermittlungsleiter | |
| | Security Consultant | |
| | SOC Analyst Forensiker | |
| | Incident Responder | |
| Optional | AD Consultant | Backup Consultant |
| | Citrix Consultant | Virtualisierungs Consultant |
| | Netzwerk Consultant | Exchange Consultant |
| | Firewall Consultant | Datenschutz Consultant |

*Eine EDR Lösung ist für einen effektiven IRT Einsatz zwingend notwendig. Sollte zum Zeitpunkt des Einsatzes keine passende Lösung im Einsatz sein, werden Trend Micro XDR Lizenzen ausgerollt. Diese können zusätzliche Kosten verursachen.

Der akute Einsatz

| | | |
|---|--|---|
| Erste Hilfe | IRT vor Ort | IRT vor Ort |
| <p>Remote Unterstützung in der ersten Woche 24x7 Erreichbarkeit</p> <p>Incident Analyst Krisenmanager Security Specialist</p> <p>Forensik Tools für die Analyse der Netzwerk Umgebung Checklisten</p> | <p>Vor Ort Unterstützung in der ersten Woche 24x7 Erreichbarkeit</p> <p>Incident Analyst Krisenmanager 3 Security Specialists Datenschutz Specialist</p> <p>Forensik Tools für die Analyse der Netzwerk Umgebung Checklisten</p> | <p>Vor Ort Unterstützung für 2 Wochen 24x7 Erreichbarkeit</p> <p>Incident Analyst Krisenmanager 3 Security Specialists Datenschutz Specialist</p> <p>Forensik Tools für die Analyse der Netzwerk Umgebung Checklisten</p> |

Ansprechpartner

Bei Interesse oder weitergehenden Fragen steht unser Ansprechpartner Julius Höltje zur Verfügung.



Julius Höltje
Team Lead Focus Sales
Cyber Security
0151 2034 6581
julius.hoeltje@pco-online.de

Dieses Dokument stellt kein Angebot dar. Wir unterbreiten gerne ein individuelles Angebot.