GULP
experts united
Pressemeldung
September 2023

5 Tipps, um die Reaktionszeit auf einen Cyberangriff zu verbessern

Die meisten Unternehmen fühlen sich in Sachen Cybersecurity gut aufgestellt, doch fragt man sie nach ihrer Reaktionszeit im Falle eines tatsächlichen Angriffs, so schwindet die Zuversicht. Diese Erkenntnis geht aus den Zwischenergebnissen des Digitalisierungs-Checks von GULP hervor. Hier sahen sich die Befragten überwiegend gut (58 Prozent) bis sehr gut (18 Prozent) abgesichert. Doch bei der Reaktionsfähigkeit sahen sich nur noch 7 Prozent sehr gut und 38 Prozent gut vorbereitet.

Dabei sind gerade die ersten Stunden während eines Angriffs entscheidend, um Maßnahmen einzuleiten. Vor allem fünf Punkte sind wichtig, um die Reaktionszeit auf einen Cyberangriff zu verbessern.

Die richtige Unternehmenskultur ist das A und O

Eine der größten IT-Sicherheitslücken sitzt ca. 40 cm vor dem Bildschirm: Die Mitarbeitenden. Nie zuvor gab es täglich so viele Phishing-Versuche wie heute. Das bedeutet für Unternehmen, dass sie einerseits ihre Belegschaft auf das Thema sensibilisieren und andererseits eine gesunde Fehlerkultur etablieren müssen. Denn mit dem Verschweigen eines Vorfalls ist niemandem geholfen und die ersten Stunden sind essenziell für die Minimierung der Schäden. Daher sollten die Mitarbeitenden zu einem offenen und ehrlichen Diskurs motiviert sowie in der Erkennung von Phising-Versuchen geschult werden.

Vorfallreaktionsplan erstellen

Ein Vorfallreaktionsplan sollte alle kritischen Systeme beinhalten und die dazugehörigen Verantwortlichkeiten sowie die Vorgehensweise klar definieren. Das reicht von der Analyse bzw. Klassifizierung der Angriffe über das Isolieren und Trennen von betroffenen Systemen bis hin zur Einhaltung von Benachrichtigungspflichten. All das sind essenzielle Dinge, deren klare Definition im Falle einer Attacke kostbare Zeit rettet. Im Idealfall unterhalten Betriebe hierfür ein dediziertes Incident Response Team aus Experten, die

über das notwendige Wissen und die Fähigkeiten verfügen, um Angriffe effektiv zu bekämpfen.

Prävention ist der erste Schritt der Reaktion

Ein funktionierendes IT-Service-Management ist maßgeblich für kurze Reaktionszeiten. Eine genaue Aufzeichnung über alle aktuell eingesetzten Systeme, Geräte und Software ist dabei essenziell. Das ermöglicht im Angriffsfall eine grundlegende Evaluation der Gefahr. Weitere entscheidende Tätigkeiten des IT-Service-Managements sind ein tagesaktuelles Patch-Management, um Schwachstellen zu beseitigen, sowie ein stringentes Berechtigungsmanagement. So kann man Attacken einerseits präventiv begegnen, andererseits lassen sich durch eine strenge Rechtevergabe Schäden lokal begrenzen, wodurch die Schadsoftware nicht tiefer in die Systeme gelangt. Darüber hinaus ist das Führen eines Incident-Reports mit „Lessons learned“ empfehlenswert. Hier wird aufgezeigt, warum der Vorfall eintreten konnte und wie effektiv die Reaktion darauf war. Daraus lassen sich wertvolle Rückschlüsse ziehen, welche Bereiche verbessert werden müssen.

Technologische Unterstützung für den IT-Service

Technologien wie Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM) sowie Endpoint Detection and Response (EDR) kommen in vielen Unternehmen zum Einsatz. Doch etwa 80 % davon werden ineffizient betrieben, da die Grundlage eines funktionierenden IT-Service-Managements nicht gegeben ist. Nur, wenn dies gewährleistet ist, entfalten diese automatisierten Systeme ihr volles Potenzial.

GULP
experts united
Pressemeldung
September 2023

Der Blick von außen

In vielen Unternehmen herrscht Ungewissheit, ob im Falle eines Cyberangriffs externe Unterstützung angefordert werden soll. „Hier ergibt sich eine spannende Analogie. Man stelle sich vor, die Firma brennt. Der erste logische Schritt ist, jetzt die Feuerwehr zu rufen, um Personen- und wirtschaftliche Schäden abzuwenden. Bei einem Cyberangriff passiert das jedoch nicht, obwohl das Schadenspotenzial vergleichbar ist“, Daniel Heeßel, Cybersecurity Manager & Deputy Group Information Security Officer bei Randstad Deutschland und damit auch für die Unternehmenstochter GULP zuständig. „Im Falle eines Hackerangriffs ist die nötige Expertise zur Schadenabwendung enorm und es müssen in kürzester Zeit rationale Entscheidungen getroffen werden. Die Erfahrung zeigt jedoch, dass sich vor allem kleine und mittelständische Unternehmen mit diesen Beschlüssen schwer tun, da die Situation häufig emotional sehr geladen ist. Aber auch in großen Konzernen trifft man auf diese Problematik. Daher empfiehlt es sich, umgehend externe Spezialisten einzusetzen. Diese betrachten unvoreingenommen das „bigger picture“ und leiten alle nötigen Maßnahmen schnell in die Wege, um die Schäden durch diese Vorfälle auf ein Minimum zu reduzieren.“

Weiter Informationen zum Thema Cybersecurity und mehr unter: www.gulp.de

Dieser Text enthält 4.816 Zeichen.
Bildmaterial finden Sie unter: https://publictouch.de/pt-news/5-tipps-um-die-reaktionszeit-auf-einen-cyberangriff-zu-verbessern/?_thumbnail_id=1731

Über GULP:
Als ein führender Personaldienstleister in den Bereichen IT, Engineering und Life Sciences bringt GULP Unternehmen und hochqualifizierte Experten zusammen: Freelancer in Projekte, Arbeitnehmer in einen temporären Einsatz zu interessanten Unternehmen oder Mitarbeiter in Festanstellung.
Um den wechselnden Anforderungen von Kund:innen und Kandidat:innen gerecht zu werden, bietet GULP eine breite Palette an Möglichkeiten der Zusammenarbeit: Kund:innen unterschiedlichster Branchen und Unternehmensgrößen erhalten die Lösung, mit der sie flexibel planen können, ohne auf das benötigte Fachwissen zu verzichten. Kandidat:innen entscheiden sich für das Job-Angebot, das ihren aktuellen Bedürfnissen entspricht – beim Start in das Berufsleben, auf dem Weg zu einer neuen Karrierestufe, bei einer beruflichen Neuorientierung oder als Freelancer:in auf der Suche nach dem nächsten Projekt.
GULP beschäftigt derzeit über 500 interne Mitarbeitende und ist an 16 Standorten in Deutschland und der Schweiz vertreten. Das Unternehmen ist eingebettet in den Verbund der Randstad Gruppe Deutschland und gehört zur niederländischen Randstad N.V., dem größten Personaldienstleister weltweit.
Weitere Informationen gibt es unter www.gulp.de

GULP
experts united

Pressemeldung
September 2023

Ihre Presse-Ansprechpartner:

Monika Riedl
GULP Information Services
Telefon: 0049 89 500 316 558
E-Mail: monika.riedl@gulp.de

Sigi Riedelbauch
public touch – Agentur für Pressearbeit und PR
Telefon: 0049 91 23 97 47 13
E-Mail: riedelbauch@publictouch.de