CYBER SECURITY UND RISIKOMANAGEMENT

Erfahrungen, Herausforderungen und Maßnahmen bei Cyberangriffen.

ERFAHREN SIE MEHR IM INTERVIEW MIT:

KATHRIN WEBER
Geschäftsführerin
IRM Interim-Risiko-Management GmbH

PATRICK JUNG
Gründer und Geschäftsführer
ISB PLUS

IT-Risiken gehören neben den Personalrisiken zu den größten Risiken für Unternehmen sowie Staat und Verwaltung.

Vorstellung

Patrick Jung, IT-Sicherheitsberater und Gründer der Firma ISB-Plus

Kathrin Weber, Risikomanagerin und Geschäftsführerin der IRM Interim-Risiko-Management GmbH

Einleitung

Als Einstieg an alle Leserinnen und Leser haben wir einige Zahlen vom BSI aus dem letzten Lagebericht aufbereitet, *hier der Link zum kompletten Bericht.*

Es werden im Monat mehrere hundert Veröffentlichungen der erbeuteten Daten von Cyberkriminellen ins Internet gestellt. Der Höhepunkt war im November 2022 zu verzeichnen, es lagen nur in diesem einen Monat allein 360 Veröffentlichungen vor. D.h. es wurden von 360 Institutionen (u.a. Firmen, Verwaltungen, Behörden, usw.) Daten wie u.a. Dokumente, E-Mails und Kontaktdaten für jeden zugänglich im Internet zum Download bereitgestellt.
Die Lösegeldzahlungen, die für eine nicht Veröffentlichung oder Entschlüsselung von Daten gezahlt wurden, stiegen rasant an und liegen im Schnitt zwischen 200.000$ bis 300.000$ pro Quartal und das nur in Deutschland. Ein sehr lukratives Geschäft für die Angreifer, die Ziele sind hierbei vielfältig.
Die Bedrohungen betreffen Gesellschaft, Wirtschaft, Staat und Verwaltung und sind für alle Bereiche eine große Herausforderung und Gefahr.

Quelle: BSI

Aus diesem Grund haben wir das Thema Cyber Security und Risikomanagement in den Fokus unseres Interviews gestellt, da eine IT-Notfallplanung die Auswirkungen eines Cyberangriffs immens reduzieren kann.

Kathrin: Welche Arten von IT- Angriffen gibt es Deiner Erfahrung nach überhaupt?

Patrick: Ich würde 3 Arten unterscheiden, die natürlich immer abgewandelt oder kombiniert werden können.
Der Identitätsdiebstahl: Hier wird versucht eine Identität zu fälschen oder die Identität einer Person zu übernehmen. Das kann eine Identität im digitalen bspw. eine E-Mail-Adresse oder eine Webseite sein. Es wird z.B. versucht im Namen einer Person, das Opfer davon zu überzeugen Geld zu überweisen. Bekanntestes Beispiel ist der CEO Fraud, hier fordert der angebliche Chef Mitarbeiter auf, eine Rechnung zu begleichen, die Rechnung und der Absender sind natürlich gefälscht. Hierdurch werden jedes Jahr Schäden in Millionenhöhe verursacht.
WICHTIG: Der Angreifer hat hier (noch) keinen Zugriff auf die IT-Systeme des Opfers, hier liegt ein klassischer Betrug vor.
Der Technischer Angriff: Klassisches Hacking von Systemen oder der Verteilung von Schadcode. Hier ist das Ziel, Zugriff auf ein System zu erlangen, um weitere Geräte zu infizieren, Daten oder Passwörter zu erbeuten. Der Eintrittspunkt sind i.d.R. Phishing Attacken per E-Mail oder Angriffe auf Systeme mit einer aktuellen Schwachstelle, für die es keinen Patch gibt (Zero-day). Gute Beispiele sind hierfür die Sicherheitslücken Log4J (12-2021) oder Microsoft Exchange (12-2022), hierdurch konnten Angreifer die Systeme komplett unter ihre Kontrolle bringen. Des Weiteren gibt es noch DDOS (Distributed Denial-of-Service) Angriffe, hierbei wird das System bspw. eine Webseite überlastet und ist nicht mehr erreichbar.
Das Social Engineering: Hierbei ist es das Ziel physikalischen Zugang in ein Unternehmen zu erhalten, um Zugriff auf Unterlagen, PCs oder Server zu erlangen. Hierbei nutzt der Angreifer schlecht abgesicherte reale Zugänge (Raucherecke) oder gibt sich z.B. als Lieferant, Dienstleister oder Kunde aus. Durch die richtige Story kommt man in 90% der KMUs in Deutschland.

Kathrin: Es ist erschreckend, wie einfach das nach wie vor funktioniert. Gibt es auch Angriffe, die dadurch vorbereitet werden können?

Patrick: Ja, eine Abwandlung ist das Vishing, das beschreibt z.B. einen Angriff per Telefon (Voice-Phishing). Hierbei wird versucht Daten und Informationen vom Opfer zu erlangen, um einen anderen Angriff vorzubereiten bspw. eine Phishing Attacke.

Der erste Tag nach einem Cyberangriff ist das pure Chaos!

Kathrin: So ein geglückter IT- Angriff hat immense Auswirkungen auf jegliche Ressourcen eines Unternehmens oder den Staat und Verwaltungen. Wie sehen denn erfahrungsgemäß die ersten Tage nach einem solchem Angriff aus?

Patrick: Der erste Tag ist das pure Chaos! Die Auswirkungen können noch nicht abgesehen werden und die Hoffnung beim „Opfer“, das alles morgen wieder läuft, ist noch vorhanden.
Häufig werden die Experten zur Analyse des Vorfalls am zweiten Tag dazu geholt und nach den ersten Erkenntnissen schwindet die komplette Hoffnung auf eine schnelle Lösung. Es findet eine Art Awareness Schulung der Betroffenen statt, ihnen wird erklärt, dass es viele Aufgaben gibt und das ganze kein Sprint, sondern ein Marathon wird. Die ersten Analysen laufen und es wird ein grobes Bild des Angriffs und der Auswirkungen skizziert. Am dritten Tag wir das ganze Ausmaß bekannt und nun müssen Aktionspläne erstellt und Maßnahmen umgesetzt werden.

Keine Rechner/Server ohne Analyse abschalten oder löschen!

Kathrin: Welche Maßnahmen müssen umgesetzt werden?

Patrick: Ganz wichtig:

- Wie kommuniziere ich generell, meine Kontakte aus Outlook und auf dem Smartphone sind nicht mehr da. Wie erreiche ich Kunden und was sage ich ihnen? In der ersten Phase kann

niemand eine Aussage geben, wann das Unternehmen wieder arbeitsfähig ist.

- Wie sind die Angreifer reingekommen, die Suche nach Patient Zero (Erstes „Opfer“) beginnt. Diese Information ist wichtig, damit man den Ursprung der Attacke und die Sicherheitslücke identifizieren und schließen kann. Falls das nicht gelingt, könnte der Angriff wieder von vorne starten.
- Wann lief das letzte vollständige Backup? Können Systeme aus dem Backup wiederhergestellt werden? Häufig sind die Backups nicht ausreichend geschützt und werden vom Angreifer gelöscht oder unbrauchbar gemacht. Bei manchen Unternehmen sind noch Snapshots auf dem Storage System vorhanden, diesen können dann genutzt werden.
- Was passiert mit den infizierten Systemen? Hier muss entschieden werden, welche Systeme können wiederhergestellt werden und was wird neu installiert. Häufig werden in dieser Phase Altsysteme durch neue ersetzt, was definitiv sinnvoll ist, aber natürlich mehr Zeit kostet.
- Wieviel PCs oder Laptops kann die IT-Abteilung pro Tag neuinstallieren? Muss die Installation per Hand mit USB-Stick gemacht werden oder gibt es eine Softwareverteilung. Häufig ist der Server der Softwareverteilung nicht im Backup, da die Datenmenge zu groß ist. Wenn dieser Server im Backup war und wiederhergestellt und bereinigt werden kann, geht die Neuinstallation automatisiert und spart viel Zeit.
- Die Organisation der Mitarbeiter und Abteilungen ist eine große Herausforderung, vor allem in produzierenden Unternehmen.
  Wer soll vor Ort bleiben und wen schicke ich nach Hause?
- Wie erreiche ich die Mitarbeiter, wenn wieder gearbeitet werden kann?

Kathrin: Was würde sich ein IT-Sicherheitsberater in so einem Notfall an Voraussetzungen im Unternehmen/in einer Behörde für seine Arbeit wünsche, um schnell helfen zu können?

Patrick: Keine Rechner/Server ohne Analyse abschalten oder löschen! Die Rechner müssen am Strom bleiben und untersucht werden. Hierzu muss ein forensisches Image erzeugt werden.
Weitere Punkte sind:

- Eine Liste mit Kotaktdaten für den Krisenstab und der Mitarbeiter für den Notbetrieb, als on- und offline Kopie (Digital und Papier)
- Eine Liste mit allen IT-Systemen (Servern) und deren Priorität für die Wiederherstellung.
- Ein unabhängiges Kommunikationsmedium mit Kontaktdaten für Onlinemeetings und direktem Austausch per Chat.
- Ein gut geschütztes Backup mit Offline-Medien und regelmäßigen Funktionschecks.
- Eine unabhängige und separate PC-Einheit für die Bankanbindung

Die Firmen, die langfristige Verträge mit Dienstleistern und/oder über ihre Cyberversicherung Anspruch auf Unterstützung haben, sind klar im Vorteil.

Kathrin: An welchen „Notfallkoffer“ soll ein Unternehmen oder eine Behörde aus Deiner Sicht auf jeden Fall denken, wenn es um die IT-Sicherheit geht?

Patrick: Das sind aus meiner Sicht die notwendigen Basics:

- Liste mit Kontaktdaten des Krisenstabs und Notfallteams
- Kontaktdaten der Kunden
- Kontaktdaten der Behörden
- Saubere und unabhängige Laptops für das IT-Notfallteam. Hier können auch USB-Sticks mit einem bootfähigen Linux vorbereitet werden, diese können auch mit den vorhandenen Laptops genutzt werden, da ein Windows Schadcode i.d.R. nicht unter Linux funktioniert.

a. LTE-Router, Switch und Netzwerkkabel, Headsets
b. Kopie der Passwortdatenbank auf USB-Stick oder ausgedruckt

Kathrin: Und wie sieht es beim Thema der Ressourcen aus?

Patrick: Die Firmen die langfristigen Verträge mit Dienstleistern oder über ihre Cyberversicherung Anspruch auf Unterstützung haben, sind klar im Vorteil. Einen Dienstleister an bspw. einem Freitag zu bekommen, der diesen Notfall übernimmt ist schwierig und sehr kostspielig. Bei einem Incident Response Team (Analyseteam mit Forensik) mit 2 Personen sind kosten von 5000 € pro Tag nicht unüblich.

Kathrin: Was können Betroffene tun?

Patrick: Ich rate allen Kunden sich eigene Ressourcen aufzubauen oder eine langfristige Partnerschaft mit einem Dienstleister einzugehen, damit Sie in so einer Situation das richtige Know-how haben und zielgerichtet unterstützt werden können.
Durch die Verschärfung des IT-Sicherheitsgesetzes wird eine weitere Verknappung der Ressourcen von Fachkräften stattfinden. Daher ist es wichtig, jetzt schon einen festen und kompetenten Ansprechpartner, dem Sie vertrauen, zu sichern.
So können Unternehmen mit ihren eigenen Ressourcen erste Maßnahmen bereits umsetzen und einen individuellen Notfallplan gegen Cyberangriffe erstellen. Hierdurch sind sie in der Lage die ersten richtigen Schritte einzuleiten und den Angriff einzudämmen, während sie auf die externe Hilfe warten.

Meiner Erfahrung nach ist es wichtig, Übersprungshandlungen zu vermeiden, hier werden häufig Beweise gelöscht und die Analyse erschwert.

Kathrin: Wie sollte grundsätzlich im Falle eines IT-Angriffs reagiert werden?

Patrick: Meiner Erfahrung nach ist es wichtig, Übersprungshandlungen zu vermeiden, hier werden häufig Beweise gelöscht und die Analyse erschwert.

Hier eine kleine Checkliste:
1. Ruhe bewahren
2. Das Netzwerk vom Internet trennen! Der Angreifer ist darauf angewiesen, eine Verbindung zu ihren Rechnern bzw. seinem Schadcode zu haben. Die beste Option ist, auf der Firewall alle Verbindungen von und nach extern zu verbieten und das Logging zu aktivieren! Wenn das nicht geht, das WAN-Kabel am bspw. Router trennen -> alle WAN-Anbindungen sind hier wichtig, auch Verbindungen zu anderen Standorten trennen (Darkfieber etc.)
3. PCs und Server: Netzwerkkabel trennen und Systeme ohne Netzwerk **weiterlaufen lassen**, auch bei VMs (virtuellen Maschinen)
4. Backupsysteme vom Netzwerk trennen oder isolieren
5. Storage Systeme auf Snapshots prüfen, diese können bei der Wiederherstellung helfen.
6. Produktionssysteme vom Netzwerk trennen ggf. Backups erstellen (Produktions- oder Steuerungsanweisungen)
7. Zugriff auf Cloud Zugänge einschränken, insbesondere wenn dort die gleichen Zugangsdaten wie am PC benutzt werden (SSO). Die Zugangsdaten aus dem Active Directory sind bei einem erfolgreichen Cyberangriff immer beim Angreifer, d.h. alle Zugangsdaten und Passwörter sind kompromittiert!
8. Krisenstab einberufen und die Mitarbeiter informieren
9. Logdateien der Domain Controller, Mailserver und Firewall sichern, damit diese nicht überschrieben werden!
10. Hilfe durch Experten holen

Wir hoffen, wir konnten Ihnen einen kleinen Einblick in die aktuelle Thematik mit praktischen Ansätzen geben.

Bei Interesse oder Fragen zum Thema wenden Sie sich gern an:

Patrick Jung
ISB-PLUS

Mobil: +49 151 416 550 30
E-Mail: info@isb-plus.de

https://isb-plus.de

Kathrin Weber
IRM Interim-Risiko-Management GmbH

Tel: +49 40 33 313 280
E-Mail: info@interim-risiko-management.de

https://interim-risiko-management.de