



Chef-Researcher von Sophos: Omnipräsente Ransomware ist längst nicht die einzige Gefahr

Vor allem Rache, Habgier und mangelnde Achtsamkeit bedrohen die Unternehmenssicherheit von innen, sagt Chester Wisniewski

Während die Welt hauptsächlich Schutz vor Ransomware sucht, sieht Chester Wisniewski, Field CTO Applied Research bei Sophos, weitere, hohe Risikopotenziale unterrepräsentiert. Er schätzt vor allem die internen Gefahren, die absichtlich oder aus Unwissenheit entstehen, als hoch ein. „Datenschutzverletzungen aus dem Inneren geschehen entweder absichtlich, beispielsweise durch Insider-Bedrohungen, oder unbeabsichtigt, wie etwa durch unsachgemäßen Umgang mit sensiblen Daten.“ Wisniewski geht von einem derart hohen Gefahrenpotenzial aus, dass aus seiner Sicht mit an Sicherheit grenzender Wahrscheinlichkeit jedes Unternehmen mit Insider-Bedrohungen konfrontiert ist und wahrscheinlich schon einmal Opfer einer solchen Bedrohung war. Seiner Einschätzung nach sind die drei Hauptgründe für Sicherheitsvorfälle aus dem Inneren Rache, Habgier und mangelnde Achtsamkeit. Vorsätzliche Diebstähle sieht der Security-Experte am wahrscheinlichsten, wenn jemand kurz vor der Kündigung steht oder entlassen wurde.“

Das Risiko: Geschäftsführerhaftung

Das hohe Sicherheitsrisiko durch die eigenen Mitarbeitenden, inklusive der vertrauten Dritten (etwa Technologiedienstleister), steht im unmittelbaren Zusammenhang mit der strengeren Geschäftsführerhaftung für alle Unternehmen und hat seit dem neuen NIS2-Gesetz insbesondere für die Betreiber kritischer Infrastrukturen besondere Relevanz.

Chester Wisniewski betont bei der Gefahr von Innen drei Aspekte, um die sich Unternehmen und insbesondere deren Geschäftsführungen umgehend kümmern sollten:

1. **Gesetzliche Verantwortung:** Geschäftsführer:innen tragen in vielen Ländern eine gesetzliche Verantwortung für die Einhaltung bestimmter Sicherheitsstandards, insbesondere im Bereich des Datenschutzes. Wenn ein Unternehmen nicht angemessene Maßnahmen zur IT-Sicherheit ergreift und dadurch Datenverluste oder Datenschutzverletzungen auftreten, kann dies zu rechtlichen Konsequenzen für die Geschäftsführenden führen.
2. **Schadensersatzansprüche:** Wenn ein Unternehmen durch eine Sicherheitsverletzung oder Datenpanne Schaden erleidet, können Geschäftsführer:innen von den Aktionären, Kunden oder anderen Parteien für den entstandenen Schaden haftbar gemacht werden. Wenn Mitarbeitende absichtlich oder fahrlässig dazu beitragen, dass solche Sicherheitsvorfälle auftreten, könnte dies die Haftung der Geschäftsführung verstärken.
3. **Organisatorische Sicherheitsmaßnahmen:** Geschäftsführungen sind dafür verantwortlich, angemessene IT-Sicherheitsmaßnahmen im Unternehmen zu implementieren. Dazu gehören die Einführung von Sicherheitsrichtlinien, die Nutzung von Sicherheitstechnologien, die regelmäßige Überprüfung der Systeme sowie die Durchführung von Audits. Eine mangelhafte Umsetzung von IT-Sicherheitsmaßnahmen kann die Gefahr von Sicherheitsvorfällen durch Beschäftigte erhöhen und die Geschäftsführerhaftung verstärken.

Verschiedene Branchen, verschiedene Risiken und ganz oft aus Versehen

Die Gefahr einer Sicherheitsverletzung von innen lässt sich genauso wenig auf einen zentralen Aspekt reduzieren, wie vergleichsweise bei Ransomware, bei der ebenfalls eine Vielfalt von Angriffsvektoren existiert. Laut Wisniewski liegt ein Hauptfaktor für innere Security-Probleme in der Art des Unternehmens oder der Organisation, in der ein Mitarbeiter oder Dritter tätig ist.

In der Verteidigungsbranche beispielsweise handelt es sich meist um Spionage. In der Technologiebranche spielt meist der klassische Diebstahl von Geschäftsgeheimnissen die wichtigste Rolle. „In diesen Fällen ist in sehr vielen Unternehmen die Gelegenheit – sprich dass Daten in der Regel zu freizügig gespeichert werden und dass zu viele Personen Zugang zu Informationen haben – die Ursache für das Problem.“

Am häufigsten kommt es nach den Erfahrungen von Chester Wisniewski jedoch zu versehentlichen Datenverlusten. Wir alle kennen den versehentlichen Verlust von E-Mail-Adressen, wenn sie mit CC statt mit BCC versehen wurden. Auch verlorene Mobilgeräte, USB-Speicher und versehentlich freigegebene Cloud-Repositories fallen bis zu einem gewissen Grad in den Bereich der Insider-Bedrohungen.

Tipps zur Vermeidung einer Geschäftsführerhaftung



Prävention im Inneren hat andere Regeln als der Schutzschirm nach außen. Chester Wisniewski gibt vier Tipps:

1. **Tools zur Verhinderung von Datenverlusten (DLP)** sind nützlich, um versehentliche Datenverluste zu verhindern, jedoch wenig effektiv, wenn die Diebstähle absichtlich und von einer motivierten Person durchgeführt werden.
2. **Endpunkt-XDR-Systeme und Firewalls** können sowohl DLP durchsetzen als auch den Zugriff und die Bewegung von Daten protokollieren. Dies ist sowohl bei der Vorbeugung als auch nach einem Vorfall sehr hilfreich, um die forensische Arbeit zu unterstützen und den Vorfall aufzuklären.
3. **Minimale Rechtevergabe** und der gezielte Zugriff nur auf jene Daten, die man kennen muss, schützt sensible Daten.
4. **Das Zero-Trust-Modell** bietet im Vergleich zu herkömmlichen Security-Konzepten ein wesentlich höheres Sicherheitsniveau, indem es nicht nur allen Geräten und Diensten misstraut, sondern auch den Anwendern. Sämtlicher Netzwerk- und Datenverkehr wird geprüft und alle Anwender oder Dienste müssen sich eindeutig authentifizieren.

„Es ist schwer, ein Unternehmen vor den inneren Risiken zu schützen, was insbesondere an den individuellen Strukturen von Unternehmen und an der Risikovielfalt liegt,“ so Wisniewski. „Dennoch müssen Unternehmen und insbesondere Geschäftsführer:innen diese Aufgabe adressieren und bestmöglich meistern. Das gelingt aus meiner Sicht am besten durch ein integriertes Security-Ökosystem in Verbindung mit einer konsequent umgesetzten Zero-Trust-Strategie.“

Social Media von Sophos für die Presse

Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf  und 

LinkedIn: <https://www.linkedin.com/groups/9054356/>

Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lucht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198